Council of the European Union

Brussels, 13 September 2018
(OR. en)

12104/18
ADD 1

Interinstitutional File:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 September 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2018) 403 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

Delegations will find attached document SWD(2018) 403 final.

Encl.: SWD(2018) 403 final

EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 403 final

PART 1/4

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

Table of contents

Glossary

The below table explains the key terms or acronyms used in this document

Term or acronym	*Meaning or definition*
AI	Artificial Intelligence
cPPP	Contractual Public Private Partnership
CEF	Connecting Europe Facility
DSM	Digital Single Market
ECSO	European Cybersecurity Organisation
H2020	Horizon 2020 Framework Programme for Research & Innovation
HPC	High-Performance Computing
ICT	Information and Communication Technology
IoT	Internet of Things
JU	Joint Undertaking (as defined by article 187 TFEU)
LEIT	Leadership in Enabling and Industrial Technologies
MFF	Multi-Annual Financial Framework
R&D	Research and Development
R&I	Research and Innovation
SME	Small and Medium-sized Enterprise
SRiA	Strategic Research and Innovation Agenda
TFEU	Treaty on the Functioning of the European Union
NIS Directive	Directive on the Security of Network and Information Systems

1 INTRODUCTION:

1.1 Political and legal context

In September 2017 the Commission adopted the Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the EU's resilience, deterrence and response to cyber-attacks. The Communication, building also on previous initiatives[1], outlined a set of proposed actions, including, among others reinforcing the European Union Cybersecurity Agency (European Union Agency for Network and Information Security – ENISA), creating a voluntary EU-wide cybersecurity certification framework to increase the cybersecurity of products and services in the digital world as well as a Blueprint for quick, coordinated response to large scale cybersecurity incidents and crises.

The joint Communication highlighted also[2] that it is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society and democracy, to protect critical hardware and software and to provide key cybersecurity services. Europe must be in a position to autonomously secure its digital assets. At the moment, Europe is a net importer of cybersecurity products and solutions and largely depends on non-European providers.[3]

Against this background, the European Commission announced in the Communication the proposal to set up a network of cybersecurity centres of expertise with a European Competence Centre at its heart to bring together resources, overcome fragmentation of efforts across the EU and stimulate the development and deployment of technology in cybersecurity. The Commission also identified the need to take advantage of the synergies between EU civilian and defence cybersecurity markets, which share many common challenges and which call for close collaboration between both communities.

In the context of this work, the Commission launched a call for proposals under the H2020 Work Programme to pilot the creation of efficient networks of competence centres across the EU, able to jointly respond to cybersecurity industrial challenges. A call for proposals for the projects was launched on 1 February 2018 and closed on 29 May, with projects starting at the end of 2018.[4] The learnings from the projects, will inform the process of creating the future Network and Competence Centre (please see Annex 5).

The proposal announced in the Communication should help meet the ambitious goal for Europe agreed by the Heads of State and Government at the Tallinn Digital Summit to be "a

[1] The cross-border nature of cybersecurity threats and the need to tackle them at the EU level has been recognised already in 2013, when the first EU Cybersecurity Strategy[1] (JOIN (3013) was adopted. Cybersecurity, cybercrime and cyber defence have been systematically included in the Commission political priorities and key initiatives – Digital Single Market Strategy – COM/2015/0192, the European Agenda on Security – COM(2015) 185, the Joint Framework on countering hybrid threats, the Communication on Launching the European Defence Fund. , the Directive on concerning measures for a high common level of security of network and information systems across the Union, (the 'NIS Directive' - (EU) 2016/1148) and the contractual public-private partnership (cPPP) on cybersecurity C(2016) 4400 between the EU and the European Cybersecurity Organisation (ECSO); In 2017 a proposal for the European Defence Industrial Development Programme aiming at enhancing the competitiveness and innovation of the Union defence industry; underlining the importance of including cyber defence was adopted by COM in 2017. COM(2017) 294 final 2017/0125 (COD)

[2] JOIN(2017) 450 final: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU;

[3] Draft Final Report on the Cybersecurity Market Study, 2018

[4] https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-proposals-eu50-million-pilot-support-creation-network-cybersecurity

global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."[5]

At the moment the efforts of research and industrial communities are fragmented, lacking alignment, and a common mission, which may hinder and does not give impetus to the EU's competitiveness in this domain.[6]

The EU has been supporting research and innovation in the field of cybersecurity by providing funds under the Seventh Framework Programme and Horizon 2020 and has been striving to reinforce the links between research and industry through collaborative projects and by establishing the contractual public-private partnership (cPPP) on cybersecurity in 2016. The EU provides also, albeit at a very limited scale, support to pilot actions for the deployment of cybersecurity and trust solutions in areas of public interest within the CEF programme.

Cybersecurity products and services constitute an important and rapidly growing market.[7] However, Europe faces strong competition, with one study ranking Europe as a geographical entity in third place, following the United States and Asia, when considering a global perspective on cybersecurity markets. According to this study, in the top 20 of the leading cybersecurity countries from a market perspective, there are only 6 European countries.[8]

The EU's international counterparts have a clear strategy and make significant cybersecurity investment designed to increase technological and innovation capacities. They are developing competence centres bringing their assets (human, knowledge, financial) together to support their industries in the quest to become global cybersecurity champions.

The creation of the Public-Private Partnership[9] on cybersecurity in the EU was a solid first step bringing together the research, industry and public sector communities in Europe to facilitate innovation in cybersecurity and within the limits of the current financial framework eventually conclude with good, more focused outcomes in research and innovation. However, Europe can pursue a much larger scale investment and needs a more effective mechanism which would build lasting capacities, pool efforts, competences and stimulate the development of innovative solutions responding to industrial challenges for general cybersecurity technology (e.g. artificial intelligence, quantum computing, blockchain and secure digital identities) as well as cybersecurity in critical sectors (e.g. transport, energy, health, financial, government, telecom, manufacturing, defence, space).

The proposal to create European Cybersecurity Industrial, Technology and Research Competence Centre with the Network of National Coordination Centres is linked to the Commission's proposals for the next Multi-annual financial framework (MFF). It would be the main implementation mechanism for EU financial resources dedicated to cybersecurity under the proposed *Digital Europe Programme*. This programme, which is subject to a separate Impact Assessment[10], seeks to enlarge and maximise the benefits of digital

[5] 29 September 2017; conclusions by Prime Minister of Estonia Jüri Ratas
[6] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 and 5 for details)
[7] Analyses, depending on the methodology used, range from €100 billion to €600 billion in terms of global market size and 12% to 15% annual growth rate.
[8] Draft Final Report on the Cybersecurity Market Study, 2018
[9] COM/2016/0410 final: Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry,.
[10] See Digital Europe Programme IA

transformation to European citizens and businesses, reinforcing the policies and supporting the ambitions of the Digital Single Market.

The different elements within the Digital Europe Programme – besides cybersecurity high-performance computing (HPC), Artificial Intelligence (AI), deployment, digital capacity and interoperability, and Advanced Digital skills – will be mutually reinforcing: Attacks on ICT systems are facilitated by the advent of ever more powerful computing capabilities. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The adoption of AI means that systems need to be trained with large sets of data ("deep learning"), which need to be secure. Likewise, AI is likely to be part of future security solutions ("self-healing systems").All these areas will also require skilled workforce. .[11]

The network and Centre will also act as an implementation mechanism for cybersecurity under Horizon Europe, the next EU R&I Framework programme. Such a comprehensive approach would allow supporting cybersecurity across the entire value chain, from research to supporting the deployment and uptake of key technologies.

Likewise, in view of the dual-use character of many cybersecurity technologies, common priorities with the defence sector (e.g. in the areas of training, sharing industrial cybersecurity intelligence, building cybersecurity capabilities, testing and certification) and of the need to avoid double-spending, synergies need to be built between civilian cybersecurity and cyber defence research and industrial communities, in line with Member States' priorities (see section 2 of this document).

1.2 Initial Reactions from Member States

The Council Conclusions[12] adopted in November 2017, called on the Commission to provide rapidly an impact assessment on the possible options and propose by mid-2018 the relevant legal instrument for the implementation of the initiative establishing a Network of Cybersecurity Competence Centres and a European Cybersecurity Competence Centre. Member States welcomed the intention to set up a network of cybersecurity competence centres to stimulate the development and deployment of cybersecurity technologies, stressing the need to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity. Specifically with regard to the possible Centre, Member States stressed the importance of its coordinating role in support of the network.

Therefore, any Commission initiative will have to find the right balance in the governance and implementation structures to ensure effective European coordination while taking into account developments at the national level. The scope of the initiative will also have to take into account the specificities of the area of cybersecurity, which has seen an important growth in activities by both private and public actors on all levels and in which considerations of national security and of European strategic autonomy play an important role. The initiative would therefore have to also find the right arrangements to work with and support industry, academia, and the public sector while giving a clear role to Member States' authorities.

[11] Idem

[12] Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, adopted by the General Affairs Council on 20 November 2017.

2 PROBLEM DEFINITION

2.1 Problem Context

Europeans increasingly value and rely on digital technologies. Critical economic sectors such as transport, energy, health or finance have become increasingly dependent on network and information systems to run their core businesses. The Internet of Things (IoT), interconnecting objects between one another and with people through communication networks, is already a reality and it is expected to boom in the near future: billions of IoT connections are forecasted in the EU in 2020[13]. Furthermore, cyberspace is considered by military forces as the fifth domain (besides land, sea, air and space) of military activity, equally critical to European Union Common Security and Defence Policy (CSDP).[14]

While the growing digital connectivity brings enormous opportunities, it also exposes the economy and society to cyber threats. Cyber-attacks are constantly on the rise. In some Member States, it has been estimated that half of all the crimes are cybercrimes[15]. Some of these attacks have aimed at high-profile targets, including power grids, important webmail services, central banks, telecommunications companies and electoral commissions. The May 2017 "WannaCry" ransomware attack affected more than 230,000 computers in over 150 countries, impacting the operations of railways, health systems, telecoms operators and businesses across Europe. Attacks on cryptosystems are also facilitated by the advent on ever more powerful computing capabilities and will soon be even more at risk with the advent of quantum computers.

A 2016 study[16] revealed that the number of security incidents across all industries rose by 38% in 2015, which is the biggest increase in the past 12 years, while at least 80% of European companies have experienced at least one cybersecurity incident. In the third quarter of 2016 alone, 18 million new malware samples were captured, i.e. an average of 200,000 per day.

Cyber incidents cause major economic damage to European businesses, undermine the trust of citizens and enterprises in the digital society and affect citizens' fundamental rights. A 2014 study[17] estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around €55 bn) in 2013; with Germany being the most affected Member State (1.6 % of GDP). A recent report, in the aftermath of the "WannaCry" attack, estimated that a serious cyber-attack could cost the global economy more than $120bn (£92bn) – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy[18].

[13] Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, IDC and TXT, study carried out for the European Commission, 2014.
[14] https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-09-06-factsheet_cyber-defence.pdf
[15] PWC, Global State of Information Security Survey, 2016, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/
[16] Idem
[17] McAfee & Center for Strategic and International Studies, 'Net Losses: Estimating the Global Cost of Cybercrime', 2014
[18] Counting the cost – Cyber exposure decoded, Lloyd's and Cyence, 2017.

2.2 What are the problems to tackle?

The European Union has already put in place a number of policy and regulatory instruments to address fast evolving cyber threats (please see section 1.1.) and to secure its society, economy and democracy against them.

However, today the EU still lacks sufficient technological and industrial capacities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field.

Within the broader course of action defined by the cybersecurity Package, the present initiative aims to contribute to tackling the following problems related to the EU's insufficient cybersecurity technological and industrial capacities:

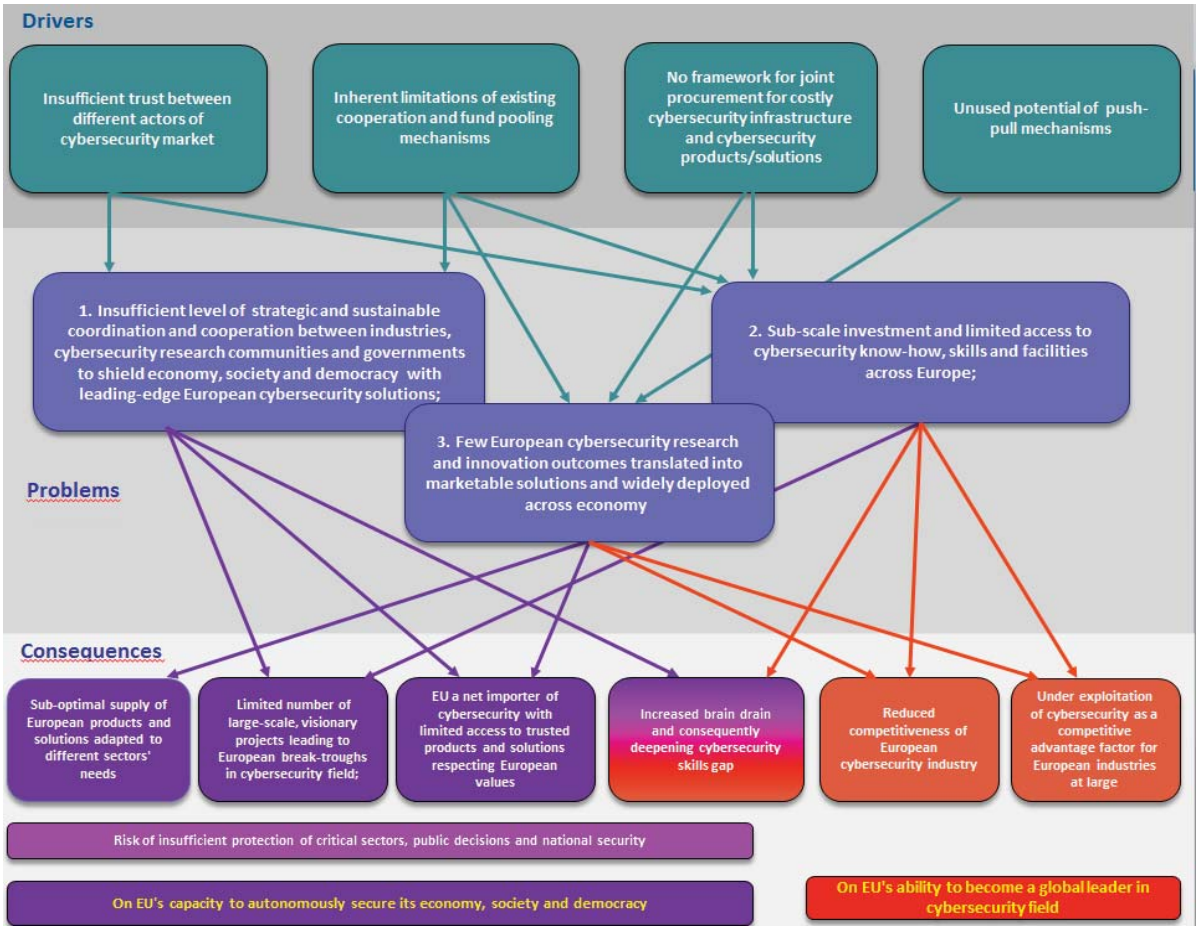
→ **Problem 1:** Insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments to shield economy, society and democracy with leading-edge European cybersecurity solutions;

→ **Problem 2:** Sub-scale investment and limited access to cybersecurity know-how, skills and facilities across Europe;

→ **Problem 3:** Few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across economy.

A problem tree portraying related problems, their drivers and consequences is presented in Figure 1 below and described in detail in the following sections.

Figure 1: Initiative Problem Tree



2.2.1 Problem 1: Insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments to shield economy, society and democracy with leading-edge European cybersecurity solutions;

→ **Insufficient cooperation between cybersecurity demand and supply industries**

European industries but also public and essential services across all sectors are subject to digital transformation. This creates security challenges, which are driving demand for security services. The businesses face the challenge of both remaining secure and offering secure products and services to their clients. The automotive industry, for example, is considering specific processes to select and implement the adequate set of cyber security solutions for each subsystem of various vehicles.[19] [20]

Yet, often businesses are not able to appropriately secure their existing products, services and assets or to design secure innovative products and services (due to e.g. lack of resources,

[19]Shifting Gears in Cybersecurity for Connected Cars, February 2017: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx

[20] See e.g.: ACEA Principles of Automobile Cybersecurity: http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

skills, access to testing facilities, different business priorities). Key cybersecurity assets (e.g. block-chain based solutions, infrastructures supporting quantum key distribution enabling highly-secure communications) are often too costly to be developed and set up by individual players.

At the same time, the links between the demand (both public and private from various sectors e.g. health, telecomm, energy, space, defence, finance, transport) and supply side of the cybersecurity market are not sufficiently well developed resulting in sub-optimal supply of European products and solutions adapted to different sectors' needs, as well as in insufficient levels of trust among market players. While some limited progress in this regard has been achieved with the establishment of the contractual Public Private Partnership on cybersecurity, this cooperation is still limited to exchange of views on the research agenda and does not seem to translate into cooperation on specific industrial challenges yet (please see also section 2.3.2).

→ **Lack of a cooperation mechanism among Member States for industrial capacity building**

At the moment there is also no efficient cooperation mechanism for Member States to work together towards building necessary capabilities supporting cybersecurity innovation across industrial sectors and deployment of cutting-edge European cybersecurity solutions. The existing cooperation mechanisms for Member States in the field of cybersecurity such as e.g. the Cooperation Group and CSIRT Network under the NIS Directive do not envisage this type of activities in their mandate. The European Cybersecurity Organisation – the Commission's counterpart in the cybersecurity cPPP has included in its governance structure an advisory committee of national public authorities. This mechanism, however, focuses primarily on providing advice on the Association's activities and exchanging best practices. Beyond presenting the public administration's perspective on the research and innovation agenda of the cPPP and exchanging good practices, the Committee does not conduct specific activities directly supporting the enhancement of cybersecurity industrial capabilities (e.g. through agreeing on common investment plans).[21]

→ **Insufficient cooperation within and between research and industrial communities**

The research community can play a vital role in supporting both industry and public authorities in meeting cybersecurity challenges. While a wealth of cybersecurity expertise and experience is available across Member States at the moment, which can make Europe a leader in the cybersecurity field, the efforts and capacities of research and industrial communities are dispersed thus hindering the EU's competitiveness in this domain.

More than 660 organisations from across the EU registered to the recent mapping of cybersecurity centres of expertise conducted by the European Commission.[22] The analysis of data shows that there are many research teams working on cybersecurity issues across the EU and that their combined efforts could allow Europe to cover the whole cybersecurity value chain. However, the results also show that there is a clear need to better coordinate the

[21] http://ecs-org.eu/documents/ecso-asbl-statutes.pdf AND http://www.ecs-org.eu/documents/uploads/591d55b9be0a6.pdf

[22] JRC Technical Reports: European Cybersecurity Centres of Expertise, 201; 660 organisations registered until 31 March 2018, when the analysis for the purpose of this Impact Assessment was been undertaken. The mapping survey has remained open beyond that date to allow as many members of the cybersecurity competence community as possible to register.

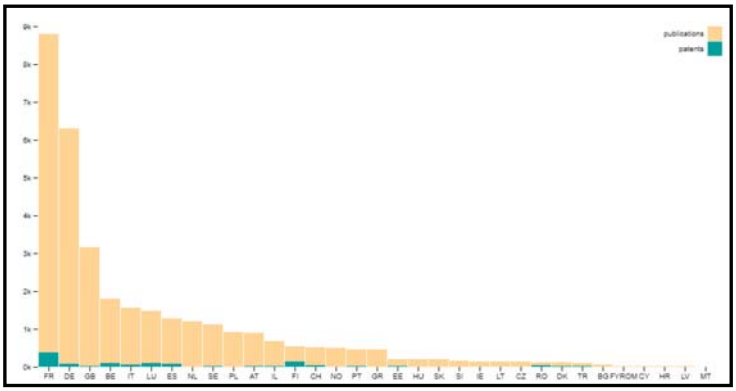
research efforts if this is to be achieved. Insufficient synergies and coordination of efforts lead to a situation in which very few major cybersecurity research breakthroughs have been reported.[23]

The results of the mapping show that many organisations working on cybersecurity issues have quite small teams. In addition, many of these expertise centres also tend to take a horizontal approach and do research across many cybersecurity domains at the same time. This often does not allow for deploying a critical mass of resources (human, financial, infrastructure) to solve specific cybersecurity challenges. At the same as they cannot invest in human and infrastructural resources, they concentrate on domains and sectors that are less demanding in terms of resources.

In consequence, despite Europe's potential to cover the full cybersecurity value chain, there are relevant cybersecurity sectors (e.g. energy, space, defence, transport) and sub-domains that are today poorly supported by the research community, or supported only by a limited number of centres (e.g. post-quantum cryptography, cybercrime research, trust and cybersecurity in AI).

Another phenomenon observed by the mapping is that European scientific excellence very often turns into publications but rarely into patents (see figure 2 below). This points towards insufficient cooperation between research and industry[24]. The consultation process demonstrated that such collaboration exists, but it is very often a short-term, consultancy-type of arrangement, which does not allow engaging in long-term research plans to solve cybersecurity industrial challenges (see Annex 2 and 4).

Figure 2 **Cybersecurity Publications/Patent ratio per country[25]**



[23] Idem

[24] While patent analysis in the cybersecurity field cannot provide the full picture of the innovation chain (e.g. it does not capture the phenomenon of software development and licensing), this piece of evidence, confirmed also by stakeholder consultation, reveals certain weakness in collaboration between the research community and the industry.

[25] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 for details)

→ **Insufficient cooperation between civilian and defence cybersecurity research and innovation communities**

The problem of insufficient levels of cooperation– both in terms of ideas and funding –also concerns the civilian and defence communities, as confirmed by evidence and consultation activities.[26]

Dual use technologies are an opportunity for the European cybersecurity market as in cybersecurity field transfers of solutions from one market to another are common practice. Unlike in other parts of the world in Europe, transfer from the civilian market to the defence market is more common. Defence clients use solutions initially developed for the civilian market.[27]

However, innovation cycles in the defence and civilian markets are relatively similar; although companies are less likely to engage in defence-oriented R&D activities without demand from Ministries of Defence. Lots of potential synergies can be identified in the experimental and development activities conducted by university research organisations and innovators (SMEs, start-ups, large players), as well as in the applied research focusing on pre-commercial development of a product. Both communities also face similar challenges related to successful transition of the technology into commercial market, which requires turning the R&D efforts into applicable and marketable product.[28]

Yet in Europe these synergies are not used to the full extent due to lack of efficient mechanisms allowing these communities to cooperate efficiently and build trust, which, even more than in other fields, is a prerequisite for successful cooperation. This is coupled with limited financial capabilities in the EU cybersecurity market, including insufficient funds to support innovation.

The fragmentation of efforts is visible, among others, at the European level as the major cybersecurity research and innovation programme – Horizon 2020 – puts clear boundaries to civilian-military cooperation. While the programme does not exclude developing and improving dual use technologies, it requires that the research activity is fully motivated by, and limited to, civil applications.[29]

Most of the 18 Member States that have responded to a recent request on cyber defence activities and needs have stressed the necessity to strengthen civil-military cooperation at EU level, notably in terms of training, education and exercises, as well as in the fields of information sharing, awareness raising and cyber defence capability development. Member States expect the EU to add value to national cyber defence efforts by supporting industry, particularly on research and development. [30]

With regard to the latter, Member States confirmed the need to reinforce synergies between civilian and military cyber research efforts, to strengthen the technological basis for cyber defence research and innovation, to promote and provide insights into technological

[26] See: Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015);: https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets; See also consultation Annex 2.

[27] Study on synergies between the civilian and the defence cybersecurity markets…

[28] Idem

[29] Article 19(2) stipulates: "Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications".

[30] EEAS, March 2018.

developments, as well as to support academic and industry R&D projects specifically in artificial intelligence.[31]

The under-exploitation of the dual use opportunities should be also seen in the context of stiff competition from global players. The EU's global cybersecurity competitors – the US, Israel and China – actively stimulate cooperation and strong synergies between civilian and military communities.[32] An informative example is the Israeli CyberSpark Industry Initiative. Supported by the Israeli National Cyber Bureau, whose mission is to build Israel's lead in the cyber field, CyberSpark managed to create an effective ecosystem for joint cyber industry activities and academia-industry partnerships[33]. The Israeli government is also supporting dual cyber R&D (e.g. through the Masad Program) to promote national and defensive cyber technologies together.[34] This coherent approach allows not only to pool public and private investment but also to attract venture capital. In 2017 Israel's cybersecurity industry raised $814.5 million in venture capital and private equity investment - a 28% over 2016 that brings the country second only to the United States.[35]

2.2.2 Problem 2: Sub-scale investment and limited access to cybersecurity know-how, skills and facilities

Despite the importance of cybersecurity on the European agenda, the current investment levels remain sub-optimal.

The EU public investment today – both at the EU and national level - including in the development and the deployment of cybersecurity technology and solutions - is below the critical mass needed to protect our economy and institutions, in particular if compared to other key international players. This has practical consequences on cybersecurity capacities of European research and industrial communities.

Public cybersecurity spending is not easily discernible from overall government spending but some available data analysis show that its levels (in terms of percentage of GDP) in Europe are low (please see Figure 3) and sub-optimal compared to other global players, who are massively investing in strategic cybersecurity programmes that are driven by public authorities with some leverage of private investments.

Figure 3: Government cybersecurity spending: a cross-country comparison over time (2008-2020)[36]

31 Idem

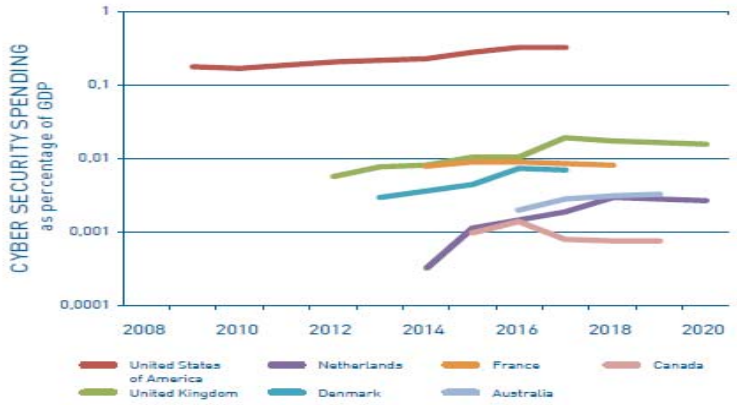
32 See for example: US Department of Defence Cyber Strategy 2015 https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

33 http://cyberspark.org.il/

34 World Development Report 2016: Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel: http://pubdocs.worldbank.org/en/868791452529898941/WDR16-BP-ICT-Sector-Innovation-Israel-Getz.pdf

35 https://www.cyberscoop.com/israel-cybersecurity-venture-funding/

36 Dutch investments in ICT and cybersecurity: putting it in perspective, *The Hague* Centre for Strategic Studies, December 2016



As an example, in the U.S.A., the government invested over USD 19 billion for cybersecurity as part of 2017 Budget (35% increase from 2016 in overall Federal resources for cybersecurity).[37] It devotes USD 760 Million in 2017 alone for cybersecurity research and innovation.[38]

At the EU level the investment in cybersecurity is channelled through different programmes of the EU budget: about EUR 600 million have been invested in cybersecurity and cybercrime projects under Horizon 2020 for the period 2014-2020 (including EUR 450 million devoted to cybersecurity cPPP for 2017-2020); the European Structural and Investment (ESI) Funds foresee a contribution of up to EUR 400 million for investments in trust and cybersecurity; about EUR 30 million were invested from CEF in the period 2014-2017.

While there is no clear picture of public investment in cybersecurity research and innovation across Member States, the reported figures from some Member States that are most active in the cybersecurity field indicate that the magnitude of the cumulative EU effort is significantly behind its global counterparts.[39] Member States are not in a position to develop individually a complete cybersecurity research and industrial ecosystem covering the full cybersecurity value chain in a competitive timeframe. While the necessary competences are available across Europe, individual Member States do not usually have the full range of know-how and most lack the necessary funding levels.

The research and industrial communities as well as the public sector in Europe struggle also with insufficient capacities and access to necessary facilities for cybersecurity experimentation, testing, and operations, which are often too large/costly for a single entity or even Member State to acquire.

During the consultation process both industrial and research communities strongly emphasised the need to reinforce the access of European industrial developers and researchers to critical-mass testing and experimentation infrastructure (e.g. quantum communication test

[37] White House, Factsheet Cybersecurity National Action Plan.
[38] The Networking and Information Technology Research and Development Program
[39] Among the Member States, who made public their investment plans: France earmarked an investment of around 165 million euros per year for cybersecurity between 2014 to 2019, with half of this budget allocated for research and innovation. The German "Self-Determination and Safety in the Digital World 2015-2020" envisages around €35 million/year for research in 4 main areas, namely High-tech for IT security, secure and trustworthy ICT systems, IT security in fields of application, privacy and data protection. In the Netherlands the vast majority of research programmes have been funded by several ministries. In 2013 which marked the second round for cybersecurity research funding, a sum of 6.4 million euros was made available by the government and public organisations.

beds; testing and penetration environment for different critical sectors, IoT environment, quantum computing facilities to validate post-quantum cryptography etc.).[40] This was supported by a comparison with the opportunities available in other markets (especially the US), where industry, researchers and public sector actors have access to real time data and testing facilities to advance their projects and get them to the market.

This challenge is also well-portrayed by the results of the mapping of Europeans cybersecurity centres of expertise. The analysis of the mapping respondents' declared activity shows that among key cybersecurity field of applications (HPC, AI, quantum etc.) that are poorly investigated at the European level are those that require deploying a critical mass of resources (see Figure 4). Looking at the distribution of the research from a sectorial perspective (see Figure 5), it is also clear that the sectors requiring costly facilities to perform experimentation and testing (e.g. energy, space, defence) are well covered only by those Member States, which traditionally have more resources available to invest.[41]

Figure 4 - Distribution of applications and technologies per country[42]

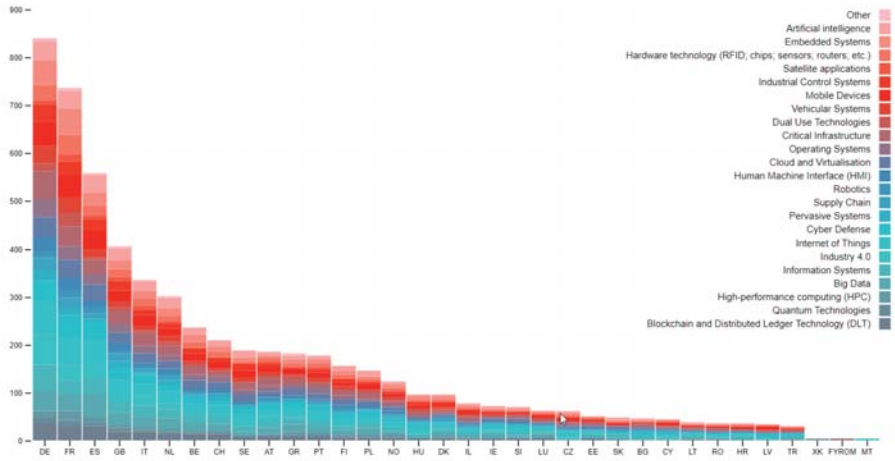
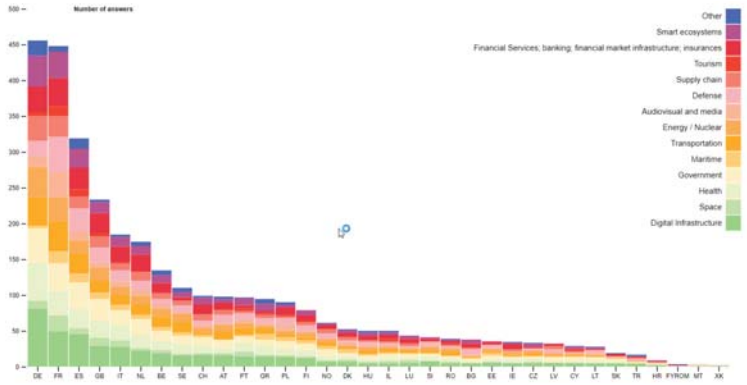


Figure 5 - Distribution of sectors per country[43]

[40] See Annex 2 on Consultation outcomes
[41] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 and 5 for details)
[42] Idem
[43] Idem



The lack of access to such facilities is also a challenge for the industrial community. Within the cybersecurity supply industry, a very substantial part of innovation is driven by SMEs and start-ups. If they cannot test their ideas, they are likely to either turn towards less costly domains and technologies or to look for opportunities outside the EU. Either option is not opportune for the European cybersecurity competitiveness. An indirect consequence can be also the loss of know-how and brain-drain as innovators decide to move outside Europe to find an ecosystem allowing them to pursue their ideas.

This is also a challenge for other industries undergoing digital transformation, including but not limited to the sectors covered under the NIS Directive (i.e. transport, energy, banking, financial market infrastructures, health, water, as well as digital service providers). However, for businesses looking at cybersecurity as just one feature of their product, it is important to be able to use such capacities when needed, without the necessity to invest heavily in the area, which is not part of their core business.

Europe also lacks a culture of investing in cybersecurity. There are many innovative SMEs in the field but they are often unable to scale up their operations due to the lack of easily available funding to support them in the early phases of development. In a public consultation conducted by the European Commission, 75% of respondents stated they did not feel they had sufficient access to financial resources to finance cybersecurity projects and initiatives.[44]

Last but not least, industrial, research and public sector (including defence) communities also struggle to find skilled cybersecurity professionals for both research and business tasks. The skills gap for cybersecurity professionals working in industry in Europe is predicted to be 350 000 (globally 1.8 million) by 2022. This is coupled with huge global competition for talent. Two-thirds of the European security professionals surveyed for the 2017 Global Information Security Workforce Study said there was too few staff available in their field, a proportion in line with the worldwide figure, which rose from 62 percent worldwide in 2015.[45]

While there are opportunities for employment and European citizens who want to learn and/or specialize in cybersecurity can nowadays access almost 500 university courses and trainings across Europe[46], the non-alignment of curricula and lack of European certification mechanism for cybersecurity professionals further complicates the situation as it is difficult for potential

[44] SWD (2016) 215

[45] 2017 Global Information Security Workforce Study commissioned by the Centre for Cyber Safety and Education and (ISC)2, was carried out from 22 June to 11 September, 2016, and surveyed 19,641 IT security professionals from 170 countries, including nearly 3,700 respondents in Europe: https://www.isc2.org/pressreleasedetails.aspx?id=14570

[46] https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

employers to judge the skills level of professionals graduating from different types of education organisations.

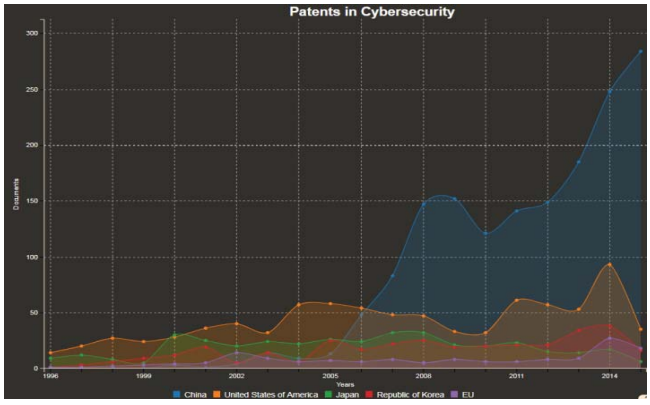
As the global competition for talent is fierce, the current lack of coordination of cybersecurity research and innovation efforts leads also to talent brain drain. Sub-optimal investment, which for talented researchers translates in practice into limited access to infrastructure as well as to large-scale visionary projects leading to European break-troughs, encourages them to look for opportunities at non-EU markets offering conditions and facilities allowing them to fulfil their ambitions.

2.2.3 Problem 3: Few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across economy

The two first problems are closely connected to the third major issue: while a lot of innovative cybersecurity research is taking place in Europe, its results often do not make it to the commercial world. And even when they do, they are not sufficiently deployed across the economy to allow the EU to become a leader neither on its own, European market nor globally.

The phenomenon of the "Valley of Death", which refers to the problematic shift from research to marketable product development[47], is of course not specific to the cybersecurity field or to Europe only. However, data suggests that European cybersecurity innovators have more difficulties to cross the Valley of Death than their competitors. The EU performs poorly, in comparison to its global counterparts, in the commercial exploitation of research outcomes. While patent analysis in the cybersecurity field cannot provide the full picture of the innovation chain[48], it shows certain trends. In fact in Europe private sector cybersecurity patenting is largely dominated by non-EU companies (see figure 6) - on average the EU owns less than 5% of cybersecurity related patents (with cryptography being the only exception with the result of 21%), while patent filing is dominated by China, followed by the USA.[49]

Figure 6: Cybersecurity Patents in Europe[50]



[47] https://www.journals.elsevier.com/technovation/call-for-papers/special-issue-surviving-the-valley-of-death
[48] E.g. the patent analysis that does not capture the phenomenon of software development and licensing); or other elements such as the cost and complexity of the patenting process
[49] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 for details)
[50] Idem

At the same time European cybersecurity products and solutions that manage to cross the Valley of Death are not widely deployed across European and global markets. The cybersecurity industry in Europe has developed largely on the basis of national governmental demand, including for the defence sector. In parallel a multitude of innovative SMEs has also emerged both in specialty/niche markets (e.g. crypto systems) and in well-established markets with new business models (e.g. antivirus software). Despite this evolving market structure companies still have difficulties growing outside their domestic, national market due to market fragmentation. As a consequence, while European companies tend to be strong and innovative, their size and capacity (mostly SMEs with few larger actors) are smaller in comparison to their US, Israeli, Chinese, South-Korean counterparts.

European companies, especially SMEs, have also little budget available for commercial development and marketing to improve their visibility across markets. They also lack sufficient resources to acquire competitive intelligence to understand where their product/service could fit in the market. This is coupled with the previously mentioned lack of EU cybersecurity investment culture with a high-risk aversion and scarcity of European venture capital willing to invest in the field.[51]

An additional issue is related to how government procurement and large tenders, which could be an opportunity for European providers to present their offer, are structured. In fact they often call for a complex package of services that single European companies (especially SMEs), unlike their global competitors, cannot provide. At the same time there is no mechanism that would facilitate swift creation of consortia of European companies that could effectively respond to such calls.

As a consequence, market leadership in the EU is in the hands of companies from third countries, which have greater resources than the EU suppliers. Despite its cybersecurity innovation potential, Europe imports 5.3% of all such products and services from outside the EU; what is more, up to 25% of the supply from within Europe is actually provided by companies with the headquarters outside Europe. At the same time major competitors (e.g. US, China) are net exporters in all cybersecurity sub-sectors.[52]

The difficulty to compete on the European and global levels often leads to mergers and acquisitions of European SMEs by non-European actors, weakening the European sector and leaving Europe also much more vulnerable and technologically dependent on others.[53]

Last but not least, it is also a missed economic opportunity. The global cybersecurity market is expected to be among the fastest growing segments of the ICT sector in the coming decade.[54]

[51] Digital SME Cybersecurity Position: https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf

[52] Draft Final Report on the Cybersecurity Market Study, 2018

[53] See: Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015); see also https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf

[54] Whereas there are differences between studies and their respective methodologies and results, one study values the cybersecurity market globally at €600 bn with an expected average growth of 17% in all the three aspects of sales, number of companies and employment in the next five years.
Draft Final Report on the Cybersecurity Market Study, 2018

2.3 What are the problem drivers?

The analysis of the evidence supporting the impact assessment identified the following main drivers contributing to the problem:

2.3.1 Driver 1: Insufficient level of trust between different actors of the cybersecurity ecosystem

For cybersecurity trust is a prerequisite of effective cooperation both between public authorities and between market actors across Europe. Thanks to the NIS Directive mechanisms and supporting non-legislative actions (e.g. cyber exercises) progress has been achieved in recent years in building trust among Member States helping to improve cooperation and information sharing at the EU level on cybersecurity issues.

However, the trust level between public authorities and the private sector from across Member States, within the private sector as well as between the private sector and the research community is still insufficient. Part of the problem is due to the fact that despite fast digitalisation of all fields of economy and society, cybersecurity is still perceived by some actors as mostly a national security issue, which should be predominantly dealt with at the national level and in smaller trusted circles. This also impacts the willingness of different actors to pool resources and invest together in developing industrial capacities (Problem 1 and 2 described above).

Some progress in building trust between actors of this European ecosystem has been achieved thanks to the Commission's initiative of creating a cPPP on cybersecurity in 2016[55], which allowed forming a sustainable platform of exchange of views between industry, research and public administration on cybersecurity research and innovation issues. However, the scale and impact of this effort is limited partially due to inherent limitations of this instrument (please see section 2.3.2).

In terms of market dynamics, the insufficient trust in the solutions offered 'cross-border' is the essential factor that clearly emerged from a number of consultations undertaken by the Commission at the time of and following the creation of the cPPP on cybersecurity.[56] As a consequence, much procurement still takes place within a given Member State and many companies struggle to achieve the economies of scale that would enable them to be more competitive both within the internal market and globally. This clearly impacts effective market deployment of European cybersecurity products and solutions (Problem 3).

2.3.2 Driver 2: Inherent limitations of existing cooperation mechanisms for highly complex cybersecurity ecosystem

The establishment of the cPPP on cybersecurity between the European Commission and the European Cybersecurity Organisation (ECSO) in 2016[57] was the first EU-wide attempt to bring together the cybersecurity industry, the demand side and the research community to

[55] Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015)
[56] See SWD (2016) 216.
[57] In its Digital Single Market Strategy for Europe(COM (2015) 192), the European Commission concluded that specific gaps still existed in the fast-moving area of cybersecurity technologies and a more joined-up approach was needed to step up the supply of more secure solutions at the European level. The establishment of a contractual public private partnership on cybersecurity to create the structural links between cybersecurity research and industrial communities aimed at stepping up work towards trusted collaboration COM (2016) 410

build the platform of sustainable dialogue and create conditions for voluntary co-investment. Public authorities, who are an important buyer of cybersecurity products and solutions themselves, have also been invited to take part in the partnership.

The partnership indeed managed to create a platform of dialogue at the EU level and by developing the Strategic Research and Innovation Agenda actively contributed to the development of the Horizon 2020 Research & Innovation Work Programme's parts related to cybersecurity. It also allowed the member organisations of ECSO to discuss other issues relevant for the cybersecurity ecosystem e.g. certification or skills development.[58]

However, the impact of the partnership on actual research and innovation activities to respond to cybersecurity industrial challenges is limited due to the inherent limitation of this cooperation mechanism. The cPPP is a light collaboration structure well-suited to federate advice on cybersecurity communities' research priorities, which can then be supported through the regular instruments of the Union's Research Framework Programme. This mechanism, however, does not envisage the possibility of implementing R&I and demonstration programmes in an integrated way[59]; it does not allow for pooling and managing budget from different sources[60] (European Commission, Member States, industry) to ensure alignment of efforts; nor does it ensure budgetary certainty to stakeholders involved that would be a clear incentive to cooperate in a structured and sustainable way on specific strategic areas. It is also not suited for ensuring the availability of shared competence and infrastructures – one of the key needs identified by the stakeholders in the consultation process (see Annex 2).[61] Last but not least, it does not sufficiently stimulate synergies between the cybersecurity civilian and military research and innovation communities given that Horizon 2020, under which rule the cPPP is created, puts clear boundaries to civilian-military cooperation by requiring that the research activity is fully motivated by, and limited to, civil applications only.[62]

These inherent limitations of the existing cooperation mechanism are an important driver for both Problem 1 and 2 hampering effective cooperation and pooling of investment necessary to enable cybersecurity communities to take advantage of know-how, skills and resources that exist across the EU.

At the same time national initiatives across a few Member States aim to bring together the competencies and industrial players in this area[63], potentially helping European companies to join forces and expand across a number of European countries. These, however, do not have the capacity to effectively link know-how and resources spread across the EU.

[58] For an overview of the ECSO working groups please see www.ecs-org.eu

[59] Ad-hoc partnerships between the participants of the cPPP are of course possible, but the contractual arrangement does not allow for the indirect management of the EU budget.

[60] While cPPP industrial partners commit to a certain level of investment, the instrument does not allow for pooling budgets together to implement projects of common interest.

[61] See Annex 2

[62] Article 19(2) stipulates: "Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications".

[63] E.g. France: Aix-en-Provence, SAFE Cluster ; Denmark: Karup, CenSec; Finland: Tampere Region, Safety and Security Cluster; Germany: Karlsruhe, secUnity; Germany: Munich, Security Cluster; The Netherlands: The Hague Security Delta

2.3.3 Driver 3: Lack for framework for joint procurement for costly cybersecurity infrastructure

At the moment there is no common European strategy to develop, acquire and ensure access of industrial, research and public sector communities to cybersecurity testing and experimentation infrastructures. As highlighted in section 2.2.2, the mapping of cybersecurity capacities across the EU shows that the sectors (e.g. energy, space, defence) and applications (e.g. HPC, AI) requiring costly facilities to perform experimentation and testing are covered to some extent only by those Member States which traditionally have more resources available to invest.[64]

Although most Member States share the same interests in advancing cybersecurity, they try to satisfy on their own, if feasible at all due to funding problems, the requirements of their national communities[65]. The specifications and procurement of the necessary equipment is done by each Member State on their own, without specific incentive to coordinate with other Member States. This solution allows some Member States to specialise in certain cybersecurity sectors or domains. This approach, however, due to the limited resources and fragmentation of the efforts, does not guarantee either the optimal coverage and access to such facilities by cybersecurity communities, nor does it constitute an economically viable solution both in terms of acquisition and optimal exploitation, as highlighted by both industrial and research communities during the consultation process.

Some Member States (e.g. Italy) are starting to consider the deployment of a public quantum communication infrastructure to secure their critical assets and communication needs, or investing in prototypes and testbeds (e.g. the Netherlands and the UK)[66]. Co-investing at EU level into the deployment of a well-interconnected quantum communication infrastructure would allow maximising the efficiency and covering many more use-cases across Europe, whilst building trust in the technology and acting as a market push for the adoption of such solutions in the private sector.

This driver directly contributes to Problem 2 and 3.

2.3.4 Driver 4: Unused potential of push-pull mechanism for effective market deployment of European cybersecurity products and solutions

The potential of a strong push-pull ecosystem between the (potentially big) demand and supply for cyber-security in Europe is far from being maximised to build up world industrial leadership in the field, ensuring autonomy and protecting our society and economy.

In the healthcare sector for example, hospitals have become incrementally digitalised while often experiencing complex and still largely un-solved security problems - partly relatedto the standards used and the lack of harmonisation of services and regulations. The potential of cybersecurity by design approach to medical devices is not sufficiently exploited either.. When new devices or systems are used, cyber security aspects should be planned and

[64] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 for details)
[65] See Annex 2 on Consultation outcomes
[66] See for example: https://www.thehaguesecuritydelta.com/projects/project/89-national-cyber-testbed

implemented and throughout the process – from the procurement, outsourcing and maintenance phases of new systems needs to be defined beforehand.[67]

In another example, cybersecurity remains a major challenge to enterprises involved in Industry 4.0 and using sophisticated digital Industrial Control Systems. For example, according to a survey carried out by Deloitte-MAPI, close to 70% of manufacturers transmit personal information via connected products, while just 55% encrypt the information they send. Challenges such as the difficulty to quantify losses from cyber intrusions, mismatching lifecycles between production machines and the IT layer, the presence of legacy industrial control systems which are more prone to cyber threats, and the risks associated to sharing data across digital supply networks call for better interaction between cybersecurity and industrial/manufacturing communities.[68]

2.4 How will the problem evolve?

The number, complexity and scale of cybersecurity incidents and their impact on economy and society are growing over time and they are expected to further increase in parallel to technological developments, for example with the proliferation of IoT devices. It is predicted that cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021.[69] A strong European cybersecurity sector is important for geo-strategic reasons. However, the three problems and related drivers described above affect EU's capacity to autonomously secure its economy, society and democracy as well as its ability to become a global leader in the cybersecurity field, allowing it to take full advantage of the opportunities presented by this fast growing ICT market.

EU's capacity to autonomously secure its economy, society and democracy

With no policy intervention strengthening cooperation mechanisms and aligning efforts, the cycle of European cybersecurity technology dependency is likely to further deepen. A closely linked consequence is the potential lack of access for European citizens and businesses to security products and solutions based on European values. An insufficient supply of European products and solutions adapted to different critical sectors' and public administrations' needs increases the risk of insufficient protection of these sectors, public decisions and might be weakening the national security of Member States. European industries and public administrations' access to cutting-edge specific and interdisciplinary know-how and testing infrastructure will continue to be limited. The lack of a clear strategy and concerted efforts to address the large cybersecurity skills gap will also leave Europe both less secure and less competitive.

In fact, as European industries have become increasingly digital, their demand for accessing innovative cybersecurity solutions will not be met in Europe and they will have to look for them outside of the EU. Adopting cybersecurity solutions from other geographies also

[67] ECSO Working Group on Sectoral Demand: Healthcare Sector Report. March 2018;

[68] ECSO Working Group on Sectoral Demand: Industry 4.0. March 2018

[69] "Global State of Information Security Survey", PwC, 2016, http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.

comprises a certain level of risk, as the technologies could be used for other purposes than purely service-related ones.[70]

Missed economic opportunities of cybersecurity supply and demand sectors

Europe is a net importer of cybersecurity products and solutions. With no policy intervention addressing the fragmentation of European efforts and sub-scale, dispersed investment in cybersecurity industrial and innovation capacities, European cybersecurity industry is not likely to be able to face fierce global competition and take advantage of this opportunity.

The lack of policy intervention is likely to leave the European cybersecurity industry (especially SMEs and start-ups) more exposed to mergers and acquisitions[71] by non-European actors, weakening the European sector and leaving Europe also much more vulnerable and technologically dependent on others. This is also closely linked with the risk of aggravated brain-drain - another side of already mentioned skills challenge.

Beyond the supply industry, cybersecurity is also a major opportunity for other European sectors and could become Europe's competitive advantage. However, without policy intervention allowing European businesses to access interdisciplinary cybersecurity knowledge and infrastructure to secure their products, Europe risks to under-exploit cybersecurity as a competitive advantage for European industries at large.

3 WHY SHOULD THE EU ACT?

3.1 Legal basis

EU action is justified based on two Treaty provisions in particular: The EU is empowered to encourage an environment favourable to cooperation between undertakings and fostering better exploitation of the industrial potential of policies of innovation, research and technological development (art. 173 of the TFEU). Furthermore, Art. 187 TFEU specifies that the EU may set up the structures needed for the efficient execution of EU research, technological development and demonstration programmes.

3.2 Subsidiarity: Necessity of EU action

Cybersecurity is an issue of common interest of the Union. As outlined in the joint Communication of September 2017[72] and endorsed by Council Conclusions[73] the EU needs to make sure that it has the technological capacities to secure its economy, democracy and society. The scale and cross-border character of incidents such as *WannaCry* or *NonPetya* are

[70] See for example: "China's ghost in Europe's telecom machine", https://www.politico.eu/article/huawei-china-ghost-in-europe-telecom-machine/.

[71] Some recent examples include the acquisition of Stonesoft (FI) by McAfee, Secusmart (DE) by Blackberry, Anubis Networks (PT) by BitSight; See also: *Cyber Security M&A Decoding deals in the global Cyber Security industry*,

[72] JOIN(2017)450

[73] General Affairs Council: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017)

a point in case. For Europe to be prepared it needs to have a thriving cybersecurity ecosystem, including industrial and research communities.

As described in the sections above, the nature and scale of the cybersecurity technological challenges and insufficient coordination of efforts within and across the industry, public sector and research communities require the EU to further support coordination efforts both to pool a critical mass of resources and ensure better knowledge and assets management. This is needed in view of the resource requirements related to certain capabilities for cybersecurity research, development and deployment (see section 2.2.2 for examples); the need to provide access to interdisciplinary cybersecurity know-how across different disciplines (often only partially available at the national level); the global nature of industrial value chains, as well as the activity of global competitors working across the markets.

None of the options analysed in this Impact Assessment go beyond what is necessary to achieve the objectives set in the following section in a satisfactory manner. Furthermore, the scope of EU intervention would not impede any further national actions in the field of national security matters.

3.3 Subsidiarity: Added value of EU action

The consultation activities carried out for this Impact Assessment (see Annex 2) confirmed the relevance of the Commission's proposal as outlined in the *Communication on Resilience, Deterrence, and Defence adopted in September 2017*. Stakeholders from the industrial and research communities considered that the Centre and the Network could add value to the current efforts on the national level by helping create a Europe-wide cybersecurity ecosystem allowing better cooperation between the research and industry communities. They also considered it necessary that the EU and Member States take a proactive, longer-term and strategic perspective to cybersecurity industrial policy going beyond research and innovation only. Stakeholders expressed the need to gain access to key capabilities such as testing and experimentation facilities and to be more ambitious in closing the cybersecurity skills gap e.g. through large-scale European projects attracting the best talents. All of the above was also seen as necessary for Europe to be recognised globally as a leader in cybersecurity.

In the consultation activities undertaken since September 2017[74] as well as in dedicated Council Conclusions[75] Member States welcomed the intention to set up a network of cybersecurity competence centres to stimulate the development and deployment of cybersecurity technologies, stressing the need to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity. Specifically with regard to the possible Centre, Member States stressed the importance of its coordinating role in support of the network. In particular with regard to national activities and needs in cyber defence, most of the Member States who had responded to a dedicated request by the European External Action Service request stated that EU added value is seen inter alia in training and education and in supporting industry through research and development.[76] The potential network and capacity building activities would indeed be implemented together with Member States or entities supported by them. Collaborations between the industry, research and/or public sector communities would bring together and

[74] See Annex 1 and 2

[75] General Affairs Council: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017)

[76] EEAS, March 2018

strengthen existing entities and efforts at not create new ones (for further information see Section 5). Member States would also be involved in defining specific actions targeting the public sector as a direct user of cybersecurity technology and know-how.

At the same time, this initiative will not target cybersecurity "operational cooperation" as governed by the NIS Directive and addressed at EU level by ENISA and the CSIRT Network set up by the Directive.

EU action is therefore justified on grounds of subsidiarity and proportionality.

4 OBJECTIVES: WHAT IS TO BE ACHIEVED?

Based on the problems identified in section 1, the following policy objectives for the current initiative have been set:

4.1 General objectives

The main policy objectives of the policy initiative are:

1. Ensure that the EU retains and develops the essential (technological and industrial) capacities to autonomously secure its digital economy, society and democracy, and that Member States benefit from the most advanced cybersecurity solutions

2. Increase global competitiveness of EU cybersecurity companies.

3. Ensure European industries have access to capacities and resources to turn cybersecurity into their competitive advantage.

4.2 Specific objectives

With the general objectives in mind, the initiative intends to achieve the following specific objectives:

1. Develop effective mechanisms for long-term strategic cooperation of all relevant actors (public authorities, industries, research community from both civil and defence areas) to set and implement a mission-driven, strategic cybersecurity agenda responding to industrial and public authorities' needs;

2. Pool knowledge and resources to provide leading-edge capabilities and infrastructures to support industry and research community in developing and validating new technologically advanced products and solutions.

3. Stimulate wide deployment of European cybersecurity products and solutions across the economy and the public sector through, among others, joint procurement.

4. Support cybersecurity start-ups and SMEs to attract investment including venture capital.

5. Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses.

4.3 Functionalities and governance of the Network and the Centre

In its September 2017 Communication, the European Commission announced the intention to set up a network of cybersecurity centres of expertise with a European Research and Competence Centre at its heart to pool resources, overcome fragmentation of efforts across the EU and stimulate the development and deployment of technology in cybersecurity. It also envisioned it to contribute to the cooperation between Member States in the area of cyber defence.

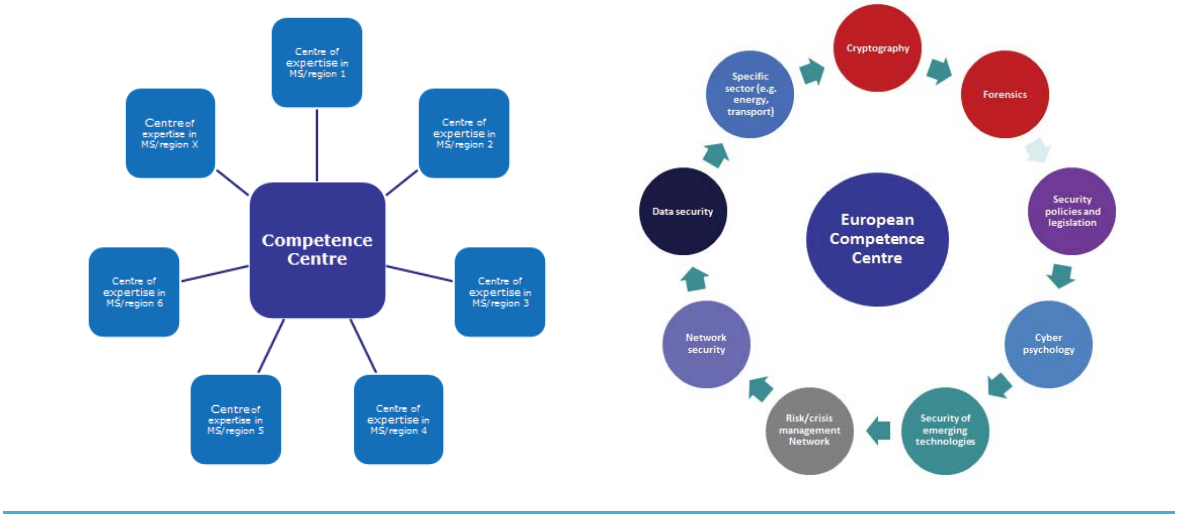
This section outlines a number of functionalities and governance elements, which will need to be taken into consideration when assessing the options for creating the Centre.

Functionality 1: Flexibility to allow different cooperation models with the network of competence centres, in line with Member States' priorities, to optimise the use of existing knowledge and resources

To facilitate cooperation between all relevant actors across Europe different network structures could be considered:

- A geographically organised network (see figure 8), which would link the European Competence Centre with one Coordination Centre per Member State creating a structure dealing horizontally with cybersecurity industrial and research challenges;
- A thematically organised community (see figure 9), which envisages supporting projects related to challenges in a specific sector or cybersecurity domain (e.g. network security, cryptography, cybersecurity of the energy sector, etc.)
- A hybrid model combining the elements of both aforementioned models

Figure 8 Geographically organised network *Figure 9: Thematically organised community*



As highlighted by stakeholders (both the industry and research communities as well as Member States)[77] during the consultation process, the cooperation model chosen will have to take into consideration the need of:

- Linking the competences spread across the EU while allowing collaboration in smaller circles (e.g. on a regional level);
- Taking advantage of existing excellence while improving capacities of Member States that might still be lagging behind;
- Interdisciplinary approach allowing combining expertise coming from different disciplines;
- Ensuring flexibility to act along the value chain to respond to fast pace and fast evolving environment;
- Encouraging long-term cooperation while leaving space for competition.

This set of diverse requirements cannot be met by Model 1 or Model 2 only. A hybrid option building on the strengths of both models should be therefore used. A "network of networks" created according to a hybrid model and supported by the Centre to facilitate cooperation and synergies, could be structured as follows:

1. **The Network of National Coordination Centres** – each Member State will nominate a national competence centre (e.g. a public body or non-profit association/cluster), which would undertake a number of tasks:

   A. **Play the hub role of a "liaison or contact point"** at the national level for the Network and the European Cybersecurity Research and Competence Centre. Some funding should be made available for these National Coordination Centres to carry out specific tasks and in particular to allow them to engage in a sustainable manner in coordination activities with both the competence centres existing within their Member States as well as with the European Competence Centre and the Network. This funding could cover costs such as e.g. human resources costs for a liaison officer(s), meeting costs, necessary coordination tools, etc.

   B. **Capacity building for the network at the national level** –identifying capacity building needs at the Member States level (e.g. in terms of investment needed in

[77] See Annex 2 and e.g. High level Roundtable with Member States, VP Ansip, Commissioner Gabriel, 5 December 2017.

testing and experimentation infrastructure at the national level, tools as well as training). In addition to their respective own national resources, the National Coordination Centres will be able to draw on EU funding in order to respond to these needs. Where economies of scale can be realised (e.g. on regional or European level), the National Cybersecurity Competence Centres would be taking active part in joint procurement activities at the European level.

C. **Acting as a one-stop-shop for national players** (public bodies, industries across different sectors, competence centres themselves) seeking advice on how to solve different cybersecurity industrial and technological challenges. The National Centre could refer a specific request to relevant players within the national network. In case of lack of specific expertise at the national level, the request could be referred to the European Cybersecurity Competence Centre to look for necessary support across the EU.

D. **Stimulating participation of national players in European and regional projects** – the National Cybersecurity Competence Centre would encourage the participation of relevant national players in European and regional cooperation projects (e.g. related to securing smart grids in a region) financed by the European Cybersecurity Research and Competence Centre.

E. **Implementing and promoting the relevant outcomes of the Network and the Centre's work** at the national level e.g. development of education/training activities following a common cybersecurity skills framework model developed by the Centre and the Network.

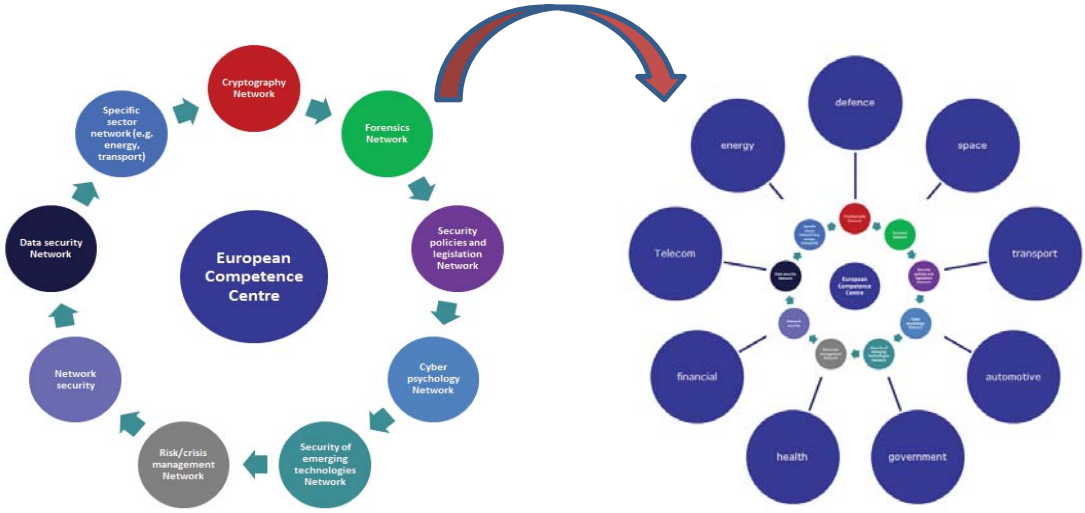
The set-up of the Network of the National Coordination Centres should allow for creating a lasting cooperation structure (going beyond the scope and duration of specific projects) and ensuring full geographic representation of the Union in key cybersecurity development activities. It should also allow identifying specific needs at the national level and upgrading the capacities across the Union. Last but not least, it allows Member States to organise their work on cybersecurity industrial and research challenges in the most efficient way taking into consideration the specificities of their system and existing structures (e.g. clusters, national networks, etc.).

2. The Community

The work, in particular with regard to capacity building and coordination, done through the **Network of National Coordination Centres** should be complemented by an inclusive Cybersecurity Competence Community**.** This Community would seek to gather all relevant European actors involved in cybersecurity technology – in particular research entities, supply-side industries, demand side industries, and the public sector. The Cybersecurity Competence Community should provide input to the activities of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network of National Coordination Centres.

Members of the Community should participate in working groups established by the Competence Centre (e.g. on specific cybersecurity domains or on specific application areas

such as energy, health, transport). Financial support to collaborative projects on such topics should be allocated following a competitive process based on scientific excellence and industrial and policy relevance. Consortia should typically include all relevant actors of the value chain (from competence centres to supply industry and user (private, public) side).



The European Cybersecurity Competence Centre would facilitate cooperation within the Community as well as between different working groups.

Beyond strategic considerations related to setting up the Network and Community outlined above, practical learnings concerning day-to-day cooperation and research agenda implementation methods used by different networks created under the H2020 Pilot projects (see Annex 6)[78] should inform the process of setting up the actual European Competence Centres Network in 2021.

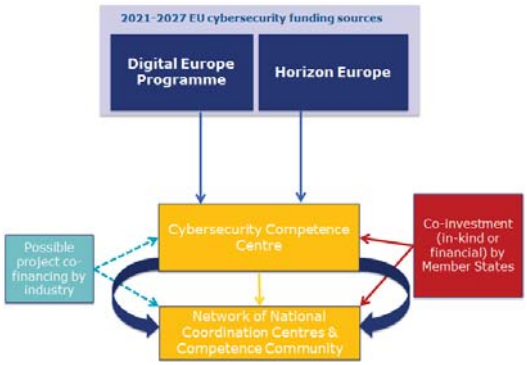
Functionality 2: The Centre as the main implementation mechanism for cybersecurity activities under a number of funding Programmes within the next Multi-annual Financial Framework (MFF)

The European Cybersecurity Competence Centre is also the Commission's proposal for the main implementation mechanism for cybersecurity industrial support activities (including deployment, investment and research) under both Horizon Europe and the Digital Europe programmes.

It is also expected that Member States will significantly contribute to the Centres' and Network's activities notably through financial and in-kind contributions.

[78] The Commission announced a call for proposals to pilot the creation of efficient networks of competence centres across the EU, able to jointly respond to cybersecurity industrial challenges. The call for proposals was launched on 1 February 2018 and will close on 29 May, with projects starting at the end of (See Annex 6 for more details)

Figure 11: Main EU cybersecurity funding sources under MFF 2021-2027



→ Functionality 3: Safeguarding the Union's and Member States' interest notably by ensuring appropriate governance structure and flexible management

Given the strategic nature of cybersecurity for European economy, democracy, society but also security the instrument should foresee the possibility for the EU represented by the Commission and to Member States to be part of its governance. This would ensure that the European Commission and Member States can play a significant role in the definition of the strategic orientation and priorities of the entity and take part in the decisions on how its budget is allocated and spent. At the same time an active role for both the private sector (representing supply and demand industries) and research communities should be possible. Last but not least the instrument should allow for flexible management to respond to the requests of different communities depending on their different needs.

The Option chosen should therefore allow the Centre to have the following governance structure consisting of the following bodies:

- The **Governing Board** should be composed of representatives of the public authorities, including the European Commission. The Governing Board should be responsible for strategic decision making, including the annual work plan and a multiannual strategic plan based on input from the Industrial and Scientific Board. The Governing Board should also have the possibility to discuss cybersecurity defence-related topics in an appropriate setting (e.g. ensuring appropriate information security and confidentiality). It is expected that Member States will significantly contribute to the Centres' activities notably through financial and in-kind contributions.
- The **Industrial and Scientific Board** will be responsible for providing input to the Governing Board in the elaboration of the annual work plan and the multiannual strategic plan. This group will be composed of members of the cybersecurity competence community and make use of the experience of the contractual PPP on cybersecurity (involving industry, scientific community, relevant public authorities and the European Commission supported by its scientific branch – Joint Research Centre).

In addition the governance and management provisions should allow for:

- Building close cooperation with the relevant existing bodies and structures such as ENISA, EUROPOL, CSIRTs Network, EDA to complement and support their action and profit from their specific knowledge. The collaboration with these entities should be defined on a case by case basis in order to profit from their evolving expertise, raise synergies and avoid duplication of resources and actions. ENISA and the future Competence Centre will engage in a structured cooperation in areas of mutual interest and in support of each other's respective mandates. In particular, the Competence Centre would be able to benefit from ENISA's experience so far with providing support to the definition of research priorities as well as its eventual market expertise from managing the cybersecurity certification scheme, while the Agency and its direct stakeholders would be among the "beneficiaries" of the outcome of the technology support to industry, research and the public sector provided by the Centre and network.

- In combination with the rules governing its "source" programmes, i.e. the Digital Europe Programme and Horizon Europe, the instrument should also make it possible to introduce provisions to protect the economic and strategic interests of the Union, i.e. protecting IPRs produced in the EU and first exploiting in Europe all EU-funded R&I results as well as to limit certain types of activities to EU-headquartered organisations only.
- Flexible approach to procuring and owning assets such as cybersecurity testing and experimentation facilities:
    - Member States should procure and own the facilities funded mainly by themselves;
    - The infrastructure co-financed from European funds across the Network should be interconnected and made available to the public and private users across Member States according to conditions defined by the Governing Body of the Centre.
    - In case of joint investment in European infrastructures and assets such as test beds, as a first step a hosting entity would be chosen – depending on the needs and capacities either in the Centre itself or in a Member State. The Governing Board should then establish the criteria for the selection of the hosting entity. The Centre and the hosting entity should sign a hosting agreement setting out the entity's responsibilities in installing and operating the infrastructure. Secondly, the Centre should launch the procedure to acquire the necessary infrastructure.

As an entity tasked with the implementation of cybersecurity-related financial support, the duration of the Competence Centre and the Network should be linked to the duration of the MFF (2021-2027). In view of the need to manage "legacy activities" launched towards the end of this timeframe, a duration of the mandate should run at least until 2029. The mandate and activities of the Competence Centre and Network should be subject to regular evaluation. A proposal to extend its mandate would need to be made for the subsequent financial framework should evaluations (see section 8) prove their effectiveness, efficiency and added-value.

5 WHAT ARE THE AVAILABLE POLICY OPTIONS?

For the right assessment of the different options it is crucial to take into consideration both the objectives and the functional requirements outlined above in order to be able to assess the effectiveness criterion.

The following options have been looked at:

1. **Baseline scenario** - Collaborative Option
2. **Option 1:** Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation
3. **Option 2:** Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities only.

In view of the general commitment already made by the Commission for the present initiative as well as in view of the important role to be played by Member States, the main distinction between the two policy options analysed lies in their scope as reflected in their legal base: an entity only based on article 187 TFEU would limit the initiative to the sphere of research and innovation, and would typically presume a financial contribution from private actors. On the other hand, an entity based on a double legal base (research and innovation as well as industry) would mean a broader mandate covering also, inter alia, industry support measures, fostering collaboration with cyber defence actors and giving a more prominent role to Member States – both in terms of their role in the governance as well as in their role as potential procurers of cybersecurity technology.

The following options have been discarded at an early stage (a brief description is presented in section 5.2):

4. No action at all
5. Network of existing competence centres only
6. Using an existing agency (ENISA, REA, INEA)

5.1 What is the baseline from which options are assessed?

5.1.1. Baseline scenario (status quo) - Collaborative Option

This scenario assumes the continuation of the current approach to building cybersecurity industrial and technological capacities in the EU through supporting research and innovation and related collaboration mechanisms under Horizon Europe.

At the moment cooperation between different types of cybersecurity stakeholders (research organizations, industry, public authorities in their capacity as buyers of cybersecurity solutions) takes place through the cPPP on cybersecurity or directly within the projects financed by the EU funds. The partnership provides a platform of dialogue and helps align efforts by developing the Strategic Research and Innovation Agenda for the Horizon 2020 Work Programme.[79] The mandate of cybersecurity cPPP is limited in time and is foreseen to be revised after 2020.

[79] JOIN (2017)450: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

The contractual Public Private Partnership is well-suited to federate advice on cybersecurity communities' research priorities, which can then be supported through the regular instruments of the Union's Research Framework Programmes.

Under this option the cooperation among expertise centres networks created through the pilot projects [80] could be further facilitated by the European Commission, possibly with the support of the cPPP on cybersecurity. However, this option assumes that the EU does not create a more robust mechanism (with relevant human and financial resources) to maintain and stimulate the network and facilitate structured cooperation between industries, public authorities, and the research community to build EU's cybersecurity technological and industrial capacities. It does not equip itself with a mechanism to effectively pool know-how and skills currently spread across the Union as proved by the mapping of cybersecurity expertise centres[81], nor creates the capacity to provide multinational project management support, testing or simulation services.

Due to inherent limitations of the cPPP legal construct (as described in detail in section 2.3.2), this option does not envisage the possibility of federating and managing budget from different sources (European Commission, Member States). This option allows industrial partners to express commitment about their individual spending (leverage factor) on areas defined in the Strategic Research & Innovation Agenda that could be further monitored by the cPPP. However, it does not envisage resource pooling for direct co-investment in e.g. necessary infrastructures or demonstration projects. The Baseline scenario entails that European industries and authorities will take up risky experimentation by themselves with their own resources and based on limited available infrastructure.

This option assumes the continuation of the support for implementing R&D projects funded through Horizon Europe but does not assume conducting activities to support the translation of the outcomes into marketable solutions nor their deployment across the market.

Last but not least this option also assumes that cybersecurity is not recognised as an area of strategic importance, which requires flexible rules to stimulate openness and exchange with other players on one hand, and to protect the Union's interest in case of work on strategic assets on the other. The cPPP's membership is open to non-EU actors. As a result the dominant, non-EU suppliers are today part of it, influencing the definition of the H2020 Work Programmes. This makes it more difficult for European market actors to develop competitive advantage.

5.2 Description of the policy options analysed in detail

Option 1 – Cybersecurity Competence Network with a European Cybersecurity Industrial, Technology and Research Competence Centre as an entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation

This option assumes creating the Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre as an EU entity with its own legal personality under art. 173 and 187 TFEU.

[80] See Annex 6
[81] See JRC Technical Reports: European Cybersecurity Centres of Expertise, 2018

This delivery mechanism would allow the Centre together with the Network, in line with the governance model discussed in section 4.3 and taking into account advice from its Industrial and Scientific Advisory Board, to respond to the needs of the industrial and other communities both from the civilian and defence sectors and support them through the following tasks that would respond to the current gaps and needs highlighted by different communities during the consultation process (see Annex 2).

I. Enhancing capabilities, knowledge and infrastructures at the Member States' and EU-level at the service of industries, public sector and research communities.

- Co-invest with Member States in upgrading and interconnecting existing national or regional equipment/tools and related skills to upscale the capacities necessary for successful development of leading-edge cybersecurity products and solutions;

- Co-invest with Member States in infrastructure and tools for European use that are not available at the moment (e.g. Quantum key distribution and facilities for post quantum cryptography). These would be made available to industrial actors across Europe, as well as to the public authorities and the network of expertise centres;

  For example, assessment and validation of the robustness of post-quantum cryptography solutions and specification of implementation modalities (minimal key length, etc.) by the industry or by members of the network will require testing these solutions against attacks run on a supercomputer or a quantum computer that could be made available through the Network and Competence Centre.

- Provide access to these infrastructures and services to a wide range of users (industry, SMEs) to address cybersecurity related industrial challenges helping them to develop innovative products and services to reach global competitiveness.

  For example, the centre and network together with stakeholders could systematically enhance the security of EU medical technologies through vulnerability assessments of medical devices, code auditing of software installed in medical systems and devices, developing innovative security controls (software and hardware) appropriate for the EU medical technologies, and developing EU profiles of all EU medical products for certification.

- Provide proactive cybersecurity technical assistance for developers, integrators and manufacturers : The research community of the Network/Centre could deliver timely and context-relevant alerts, advisories and guidance to developers, integrators and manufacturers in all industries about the cybersecurity requirements and risks of new emerging technologies (e.g. neural networks for AI deep earning, robotics, Quantum tools, satellite, virtual reality technologies) and modules (e.g. new software libraries, modules, components) that wish to use in designing future products and services. This will be an effective single point of reference for civilian and military industrial developers, integrators and manufacturers.

II. Stimulating wide deployment of European cybersecurity products and solutions

- Ensure visibility and availability of European cybersecurity products and solutions to public authorities and demand side industries (e.g. for public procurement purposes; e.g. through developing and promoting a user-friendly database of European cybersecurity

products and solutions, with information about their possible application across different domains);

- Respond to the demand created by the growing needs of fast digitising public and critical sectors (e.g. health, public administration) by working on joint procurement of leading-edge cybersecurity products and solutions;

III. Supporting cybersecurity start-ups and SMEs to attract investment including venture capital

- Develop tools and coordination mechanisms to facilitate access of cybersecurity start-ups and SMEs to venture capital (e.g. enhance visibility of cybersecurity projects/products European companies are working on; create database of venture capital funds interested in cybersecurity);
- Create a platform of cooperation for cybersecurity SMEs to connect them and foster cooperation on projects but also help them create consortia to respond to tenders and procurement offers;

IV. Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses:

- Provide appropriate input to education policy makers in order to enhance cybersecurity education in particular for the purpose of fostering high-end professional skills (e.g. by developing cybersecurity curricula in civilian and military educational systems); support the alignment, enhance and continuously assess cybersecurity professional certification programmes. Alignment of education and skills will help developing a qualified EU cybersecurity workforce – a key asset for cybersecurity companies as well as other industries with a stake in cybersecurity;
- Facilitate access by other cybersecurity and anti-cybercrime entities (Member State agencies as well as e.g. ENISA, EC3, EUROPOL, CERT-EU, Centre of Excellence for countering hybrid threats) and training centres to state-of -the art methodologies and tools (e.g. AI-analysis, simulation and Deep learning exercise platforms) to perform their operations (e.g. dynamic risk assessment and incident handling, cybersecurity/cyber defence exercises) as effectively as possible. Facilitate the necessary research focused specifically on advancing their cyber-ranges (e.g. Internet-scale simulation environments, modelling/visualization tools and virtual machines) so that interested entities can continuously help the civilian and military stakeholders to handle upcoming complex attacks and incidents and improve preparedness and resilience
- Facilitate access to specialised trainings available throughout the Network

V. Shaping and coordinating Research & Development supporting objectives of the initiative

- Shape, implement and coordinate industrial cybersecurity research and efforts towards a common, continuously evaluated and improved EU cybersecurity research agenda. Act as a single delivery mechanism for different funding programmes (Horizon Europe, Digital Europe Programme) and enhance synergies in relation to the European Defence Fund;

- In collaboration with the industry and the network, support a number of specific large research and demonstration projects in key next generation digital technological capabilities (including e.g. Artificial Intelligence, High Performance Computing, Virtual technologies, Quantum Communications, Post-quantum Encryption).
- Solve sector-specific cyber security industrial challenges: collaborate with industrial stakeholders to identify sector-specific (e.g. automotive, energy, transport, finance, governmental, telecom, defence, transport, space) cyber security needs requirements and challenges; develop and support cyber security research roadmaps for all sectors.

  For example, the centre with the members of the network could address the cybersecurity of connected, autonomous vehicles by developing penetration test beds for assessing the security risks and vulnerabilities of prototypes, developing innovative reference architectures, and providing a consistent set of cybersecurity guidelines across the manufacturing and connectivity value chain.

  For example, a cyber defence dimension could include supporting Member States' development of common capabilities, facilitating joint cyber defence training, exercises and testing, and supporting work on cyber defence taxonomies and standards, in line with priorities commonly agreed by Member States within the EU.[82]
- Support research to facilitate and accelerate certification processes[83] (e.g. build new certification methodologies and easy-to-use auditing tools).
- Develop knowledge management tool to ensure that the industrial community is able to access and take advantage of the expertise represented in the network.

Governance and management

The body would have its own governance structure, staff and a dedicated budget. The suggested legal base allows for the creation of the public-public governance structure with an important advisory role of the private sector and the research communities. It also allows pooling contributions and resources from both the Union and Member States and could also envisage contributions from the industry, where approporiate.

Experience from other bodies based on the same Treaties provisions shows that this model allows as well for flexible set-up of cooperation with the network[84], including the different possible structures discussed in section 4.3 – namely, a network organised along geographical lines, a Community organised along thematic lines, or a combination thereof.

[82] Further potential tasks with regard to defence are discussed in JOIN(2017)450.

[83] These activities would be without prejudice to the General Data Protection Regulation and in particular to its relevant provisions regarding certification.

[84] See example of the Knowledge and Innovation Communities and their relationship with the European Institute of Innovation and Technology.

5.2.1 *Option 2 – Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities*

This option assumes creating the Network of Competence Centres with the Cybersecurity Research and Competence Centre as a Union Body established under Art 187 TFEU[85] that can be used for the indirect management of the EU budget.[86]

Under this option the Centre together with the Network could implement the following types of tasks that would respond to the current gaps and needs highlighted by different communities during the consultation process.

I. Shaping and coordinating Research & Development:

Under this option shaping the research efforts would focus on civilian communities. The Centre together with the Network could do the following tasks:

- Shape, coordinate and support cybersecurity research towards a common, continuously evaluated and improved EU cybersecurity research agenda.
- In collaboration with the network and the industry, support a number of specific large research and demonstration projects in key next generation digital technological capabilities (including e.g. Artificial Intelligence, High Performance Computing, Virtual technologies, Quantum Communications, Post-quantum Encryption).
- Solve sector-specific cyber security industrial challenges: collaborate with industrial stakeholders to identify sector-specific (e.g., energy, transport, finance, governmental, telecom, defence, transport, space) cyber security needs requirements and challenges; develop and support cyber security research roadmaps for all sectors.
- support research to facilitate and accelerate certification processes (e.g. build new certification methodologies and easy-to-use auditing tools).
- Develop knowledge management tool to ensure that the community is able to access and take advantage of the expertise represented in the network.

II. Enhancing EU-level and Member States' research capabilities, knowledge and infrastructures to support research and industrial communities as well as public authorities:

- Co-invest with Member States in upgrading and interconnecting existing national or regional research equipment/tools and related skills to upscale the capacities necessary for conducting leading-edge cybersecurity research activities.
- Co-invest with Member States in research infrastructure and tools for European use that are not available at the moment. They would then be made available the network of expertise centres and industrial actors across Europe (e.g. facilities for post quantum cryptography).
- Provide access to these infrastructures and services to a wide range of users (research

[85] A JU is established by a Council Regulation, taking into account the opinion of the European Parliament and the European Economic and Social Committee

[86] In accordance with Art 58.1 (c)(iv) of the Financial Regulation (FR). Indirect management means that funding programme is implemented by a third-party organisation (e.g. public-private partnership in the form of a Joint Undertaking) and not by the EU institutions, executive agencies or Member States themselves. See: http://ec.europa.eu/budget/explained/management/managt_who/who_en.cfm

organisations, industry, SMEs) to conduct research related to cybersecurity challenges.

- Provide proactive cybersecurity technical assistance for developers, integrators and manufacturers. The research community of the Network/Centre could deliver timely and context-relevant alerts, advisories and guidance to developers, integrators and manufacturers in all industries about the cybersecurity requirements and risks of new emerging technologies (e.g. neural networks for AI deep earning, robotics, Quantum tools, satellite, virtual reality technologies) and modules (e.g. new software libraries, modules, components).

III. Support closing the cybersecurity skills gap

- Helping to align cybersecurity skills programmes and adapting them to specific sectorial needs, which could serve as an input to education policy makers;
- Coordinating and facilitating necessary research to improve and advance training courses offered by different educational organisations to help them adapt programmes to constantly evolving and complex cybersecurity challenges; Facilitating access to specialised trainings available throughout the Network

Governance and features

An entity set up under art.187 TFEU is an autonomous EU legal entity, with its own budget, staff, structure, rules and governance that can be tasked to implement actions under Framework Programmes (e.g. H2020 or CEF under current budgetary perspective). It can combine budget with other sources of funding (national, private) allowing the implementation of Research & Innovation and demonstration programmes in an integrated way. It gives a key role to industry as the main partners of the Commission.

Experience from other bodies based on the same founding regulations – typically Joint Undertakings – shows that this model allows as well for a flexible set-up of cooperation with the network[87], depending on the final decisions that will be taken by co-legislators related to how the network should be structured and interact with the Centre (please see section 4.3). However, given the civilian character of the EU R&I Framework Programmes, such an entity would not be best placed to create synergies with the defence sector.

An entity limited to supporting research and innovation can carry out procurement procedures for infrastructures, necessary to support research and development activities (typically such a structure has its own procurement and financial rules adopted by the Governing Board). Established as a Union body, it can benefit from VAT and excise duties on its purchases in all EU Member States and may adopt procurement procedures not subject to the Directive on public procurement as implemented in national law.

This option would limit the intervention to the area of research and innovation. The capacity of such an entity to support the large-scale deployment and take up of new secure technologies through the Digital Europe Programme or any other programme would be limited.

[87] See example of SESAR Joint Undertaking: http://www.sesarju.eu/

5.3 Options discarded at an early stage

5.3.1 No action at all

This option would mean stopping all public support at the European level for research, innovation and industrial development in cybersecurity field. The option is discarded because it is contrary to key strategic documents, including the 2013 EU Cybersecurity Strategy, the Joint Communication of September 2017[88] as well as supporting Council Conclusions[89], which point to a clear vision set by the Heads of State and Government at the Tallinn Digital Summit for Europe to be "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."[90]

5.3.2 Network of existing competence centres only

This option assumed that the delivery mechanism does not include any common governance structure to coordinate network activities. Partner organisations would simply cooperate to achieve a common goal based on programming documents and mutual agreement. Without a centre, there would be a lack of a focal point that would ensure accountability of all responsibilities taken by the network.

This type of networks has already been implemented in a number of projects financed under past Framework Programmes. Such collaboration can be quite effective in achieving the desired goals within their scope, but their sustainability beyond project timeline is very limited and knowledge management mechanisms allowing to take advantage of their outputs are insufficient. For example, the instrument of "Networks of Excellence", introduced with FP6, was discontinued under FP7. An independent expert group identified "achieving 'durable integration' and creating joint organisational arrangements and structures (…) the major problems for achieving the core objectives of NoEs."[91]

This option would focus the intervention on the capacity-building and ecosystem-building aspects at the regional and national level with limited positive impact in terms of reducing fragmentation and sustainable knowledge and capacity sharing at the European level. Without a central implementation mechanism and project manager, the procurement of particularly costly infrastructure and pan-European solutions would be practically impossible, and cooperation in this regard would likely be limited to bilateral or multilateral cooperation between larger and more advanced Member States, if at all.

5.3.3 Using an existing agency

This option would assume conferring the tasks of the Competence Centre to one of existing agencies – either ENISA or one of the executive agencies - Research Executive Agency (REA) or Innovations and Networks Executive Agency (INEA).

The option of using ENISA was discarded on the basis of a mismatch between the objectives, the desired functionalities of the Competence Centre and the mandate and related structure of

[88] JOIN(2017)450.

[89] General Affairs Council: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017)

[90] Conclusions of the Prime Minister of Estonia Jüri Ratas after the Tallinn Digital Summit, 29 September 2017

[91] An example of the Network of Excellence on cybersecurity was SYSSEC. Counting over 80 members, it was considered very successful. However with the end of the grant, also operations ended.

ENISA (current, as established by Regulation of 2013[92], and future, as proposed by the Commission in September 2017[93]). In particular:

- ENISA is a decentralised EU Agency founded on the basis of article 114 of the TFEU. Its focus on policy advice and facilitation of operational cooperation is not suitable for the mission of the Centre. Furthermore, its mandate is limited to internal market issues, which leaves e.g. any defence issues out of the scope of its action.

- The tasks entrusted to ENISA, mostly focused on strategic advice on regulatory issues (support to EU policy development and implementation), capacity building and operational cooperation to prevent and respond to cybersecurity incidents are meant to satisfy different needs than the Competence Centre, with a strong focus on support to industry, research and development and public procurement.

- In order to support its objectives of enhancing cooperation and coordination at EU level, the structure of ENISA, as confirmed by the impact assessment supporting the current proposal for the new mandate, needs to stay "agile" and leverage on the EU and Member States' competences. The Commission proposal opted for a structured cooperation between ENISA and the other EU bodies with competences/stakes in cybersecurity.

(Section 4.3 discussed the possible future relationship between ENISA and the cybersecurity competence centre and the network.)

The option of entrusting the tasks to the Research Executive Agency (REA) or Innovations and Networks Executive Agency (INEA) was discarded at an early stage due to a number of factors. Firstly, the governance of these Agencies does not allow for active participation of Member States. This is a disqualifying factor given that cybersecurity is perceived by many Member States as a field closely linked to national security. This would hamper achieving the objectives of the initiative (e.g. pooling resources). Secondly the tasks of the Network and Competence Centre as requested by stakeholders in the consultation process should go largely beyond managing EU funds for cybersecurity only, which is the core mandate of executive agencies. General purpose agencies such as REA and INEA could not nurture a specific in-depth cybersecurity expertise required by the Centre in a sustainable manner.

6 WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section analyses the economic, environmental and social impact of the options as compared to the baseline scenario, in line with the Better Regulation Guidelines together with the coherence with other policy and the views of stakeholders.

6.1 Option 1: Cybersecurity Competence Network with a European Cybersecurity Industrial, Technology and Research Competence Centre entity empowered to

[92] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

[93] Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU)526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"); COM(2017) 477)

pursue measures in support of industrial technologies as well as in the domain of research and innovation

Effectiveness

Objective 1: Develop an effective mechanism for long-term strategic cooperation of all relevant actors (public authorities, industries, research community from both civil and defence areas) to set and implement mission-driven cybersecurity agenda responding to industrial and public authorities' needs;

A significant positive impact on improving coordination and alignment of the efforts is expected under this option as the suggested mechanism - with its own budget and human resources – should allow sustainably facilitate the efforts of all relevant communities (demand and supply side industry, public administration, research communities from both civilian and defence fields).

The suggested mechanism is suited for supporting a wide range of the Network's, community and own activities supporting industrial development (e.g. pooling resources and procuring and co-investing in infrastructure, in particular for testing, experimentation and certification, supporting deployment activities, skills development, etc.) as well as for implementing a strategic research agenda responding to industrial needs.

It can also act as a single implementation mechanism for cyber security -related financial support from the Digital Europe Programme and Horizon Europe programmes, and enhance synergies between the civilian and defence dimensions of cybersecurity in relation to the European Defence Fund.

In conclusion, the entity as described under Option 1 is effective to achieve Objective 1.

Objective 2: Pool knowledge and resources to provide leading-edge capabilities and infrastructures to support industry and research community in developing new technologically advanced products and solutions.

The mechanism suggested under Option 1 allows for pooling public and private resources to co-invest with Member States in upgrading available capacities and invest in developing assets that are still missing (e.g. facilities for post quantum cryptography) and which could then be made available to the industrial actors across Europe as well as to public authorities and the research community. In conclusion, Option 1 is effective to achieve Objective 2.

Objective 3: Stimulate wide deployment of European cybersecurity products and solutions across the economy and the public sector through, among others, joint procurement.

As described in section 5.2.1, the Option 1 allows to conduct activities supporting wide deployment of European cybersecurity products and solutions across the market helping Member States shield their economies and societies against cyber threats on one hand and increasing competitiveness of the European cybersecurity industry on the other (e.g. by working on joint procurement of leading-edge cybersecurity products and solutions in response to growing demand from fast digitising public and critical sectors such as e.g. health, public administration; conducting activities ensuring visibility of European cybersecurity products to the demand side industries, supporting access of SMEs to public procurement and venture capital). In conclusion, Option 1 is effective to achieve Objective 3.

Objective 4: Support cybersecurity start-ups and SMEs to attract investment including venture capital.

As described in section 5.2.1, Option 1 allows conducting activities start-ups and SMEs to attract investment to turn their research ideas into a marketable product or solution. Given that access to funding is one of key challenges for the European cybersecurity SME and start-up community, the mechanism is likely to improve the situation by helping the community gain visibility towards potential investors. This should help retain the know-how and business competences in Europe and avoid brain-drain of specialists, who currently need to look for opportunities to develop their ideas outside the EU. In conclusion, Option 1 is effective to achieve Objective 4.

Objective 5: Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses.

As described in detail in section 5.2.1, Option 1 allows to complement the efforts of the Member States by providing appropriate input to education policy makers in order to enhance cybersecurity education (e.g. by developing cybersecurity curricula in civilian and military educational systems but also input for basic cybersecurity education); The Option would also allow supporting the alignment and continuous assessment of professional cybersecurity certification programmes - all necessary activities to help close cybersecurity skills gap and facilitate industries' and other communities' access to cybersecurity specialists. The Option also allows supporting targeted research to enable other cybersecurity entities and training centres to have state-of -the art methodologies and tools to advance their cyber-ranges and therefore improve preparedness and resilience to cyber-attacks. In conclusion, Option 1 is effective to achieve Objective 5.

Efficiency/ Impact on economy, competitiveness, competition and SMEs

The Option 1 scenario would have a positive impact on the EU's competitiveness and SMEs as it assumes creating a mechanism capable of building Member States' and Union's cybersecurity industrial capacities and effectively translating European scientific excellence into marketable solutions that could be deployed across the economy.

This option allows pooling resources to invest in necessary capacities at the Member States' level or develop European shared assets (e.g. by jointly procuring necessary cybersecurity testing and experimentation infrastructure). These assets could be used by industries and SMEs across different sectors to ensure that their products are cybersecure. This is likely to result in:

- Increased access of SMEs and industries from different sectors to such facilities, which will stimulate innovation, allow translating research results into real products and solutions and shorten the development processes. This will also cut costs for some demand-side businesses, who would not have to either invest in their own testing facilities or look for them outside Europe;
- Through support for capacity and ecosystem-building at national level and within thematic networks: better market insights and more contact with potential business partners for SMEs.
- Through support to demand-supply articulation: better market opportunities for SMEs
- Further turning cybersecurity into a competitive advantage factor for European industries at large;
- Allowing Member States to make investment economies thanks to coordinated efforts with other interested Member States;

The scenario also envisages mechanisms to support market deployment of cybersecurity

products and solutions. While respecting the rules of fair competition, these activities would help the European cybersecurity industry to overcome current market barriers and increase their market share. In the mid-term this should help Europe reaching import-export balance as far as cybersecurity products and solutions are concerned and in the longer-term become a net exporter in the field.

This scenario also allows taking advantage of the dual-use market opportunities by allowing the defence and civilian communities to work together on shared challenges.

This option is also likely to add-value to the national efforts of addressing cybersecurity skills gap – a challenge not only in terms of securing economy but also a key resource for European industries to ensure their competitiveness.

At the EU level, this option also allows to improve coherence and synergies between different funding mechanisms (Digital Europe Program, Horizon Europe) and reduce administrative burden of managing different cybersecurity funding programmes. Pooling resources will also help to achieve the economies of scale and help avoid double-spending.

This option does not foresee any new regulatory obligations for businesses. At the same time the businesses and especially SMEs are likely to reduce their costs related to their efforts in designing innovative cyber secure products.

In conclusion, the Option 1 scenario has clear positive impact on economy, competitiveness, competition and SMEs, much higher than that of the baseline scenario. It is also likely to substantially increase Member States' capacities to autonomously secure their economies, including protecting the critical sectors, increasing competitiveness of European cybersecurity businesses as well as industries across different sectors, which will be able to appropriately secure their existing assets and design secure innovative products while reducing security related R&D costs. This should ultimately allow the EU to become a leader in the next-generation digital and cybersecurity technologies.

Social and Environmental Impact

This Option is likely to have a positive impact on the social sphere. It will allow public authorities and industries across Member States to more effectively prevent and respond to cyber threats by offering and equipping themselves with more secure products and solutions. This is in particular relevant for the protection of access to essential services (e.g. transport, health, banking and financial services).

Increased capacity of the European Union to autonomously secure its products and services is also likely to help citizens enjoy their democratic rights and values (e.g. better protect their information-related rights enshrined in the Charter of Fundamental Rights, particularly the right to the protection of personal data and private life) and consequently increase their trust in the digital society and economy.

No specific or major impact on the environment is expected under this scenario. However, an indirect positive impact could be achieved through developing specific cybersecurity solutions for sectors having potentially huge environmental impact (e.g. nuclear power plants). This could help avoid potentially devastating consequences of cybersecurity attacks on this type of infrastructure.

Stakeholder support

The majority of industrial and research community stakeholders consulted argued in favour of setting up a mechanism allowing the EU to have a coherent cybersecurity industrial policy to stimulate the development of capacities allowing Europe to autonomously secure its economy, society and democracy (please see Annex 2 on Consultation outcomes). Stakeholders used the following key arguments:

- The cybersecurity support under next MFF should go beyond research and development activities only combining also market deployment activities;
- The Centre and the Network could add value to the current efforts at the national level by:
    - Helping create Europe-wide cybersecurity ecosystem allowing to cooperate public authorities, industries and research communities from both civilian and military sectors;
    - Helping the community work with a longer-time, strategic perspective;
    - Ensuring access to industrial and research communities across Europe to key capabilities such as testing and experimentation facilities;
    - Helping achieve interdisciplinary approach to cybersecurity in Europe and becoming a knowledge management platform, which could be used by the whole cybersecurity community;
    - Helping close the cybersecurity skills gap and preventing brain drain by offering interesting challenges for European researchers (e.g. large-scale, ambitious European projects attracting highly-skilled people).
    - Ensuring visibility of European cybersecurity know-how and competence both within the EU and globally;

At the same time, stakeholders emphasised that the key to success will be a well-defined role of the Centre and an inclusive, collaborative approach to the Network to avoid creating new silos. The structure should also be flexible so that it can be easily adapted given that cybersecurity is a fast-pace environment.

6.2 Option 2: Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities

Effectiveness

Objective 1: Develop effective mechanism for long-term strategic cooperation of all relevant actors (public authorities, industries, research community from both civil and defence areas) to set and implement mission-driven cybersecurity agenda responding to industrial and public authorities' needs;

The mechanism suggested under Option 2 (based on art. 187 of TFEU) due to its nature (legal entity with its own staff, budget, structure, rules and governance) is likely to have a positive impact on achieving better coordination of the efforts of a wide range of stakeholders (public administration, demand and supply side of the industry, research communities). However, given the nature of the research programmes for which this instrument is dedicated, it would be possible to involve the defence community in this cooperation only to a very limited extent and only for work on civilian cybersecurity applications. This instrument does not allow for coordinating activities going beyond research and development only e.g. supporting market deployment of cybersecurity products and solutions, nor would it allow the involvement of actors from cyber defence. In conclusion, such an entity is partially effective to achieve Objective 1.

Objective 2: Pool knowledge and resources to provide leading-edge capabilities and

infrastructures to support industry and research community in developing new technologically advanced products and solutions.

As described in section 5.2.2, an entity limited to supporting research and innovationallows for pooling public and private resources to co-invest with Member States in upgrading available capacities and invest in developing assets that are still missing at the European level and which could then be made available to the public authorities, the network of expertise centres and industrial actors across Europe; The use of these resources should be, however, limited to research and development activities. In conclusion, such an entity is partially effective to achieve Objective 2 given the limitation related to the purpose for which improved capacities could be used.

Objective 3: Stimulate wide deployment of European cybersecurity products and solutions across the economy and the public sector through, among others, joint procurement.

An entity limited to supporting research and innovation could not implement the tasks related to stimulating deployment of cybersecurity products and solutions in view of the limitations imposed by the Treaty legal base. This means that the Centre could not support e.g. joint procurement of leading-edge cybersecurity products and solutions nor other activities encouraging market deployment. In conclusion, Option 2 is not effective to achieve Objective 3.

Objective 4: Support cybersecurity start-ups and SMEs to attract investment including venture capital.

An entity limited to supporting research and innovationcould support these tasks as long as they concern financing for research and development and not for marketing and deployment of products and solutions across the market. Given that access to funding, including venture capital, is one of the weaknesses of the European cybersecurity ecosystem, the Centre is not likely to substantially improve this situation as investors are looking for business opportunities rather than for the research outcomes only. Such an entity is therefore effective to achieve Objective 4 to a very limited extent.

Objective 5: Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses.

An entity limited to supporting research and innovationcould have a positive impact on closing the cybersecurity skills gap as it would be in a position to carry out targeted research to enable other cybersecurity entities to improve their training and cyber ranges. However a whole range of tasks related to aligning cybersecurity skills curricula and assessing the cybersecurity professional certification programs would fall outside the scope of the Centre due to the mandate limitations imposed by the EU Treaties. In conclusion such an entity is partially effective to achieve Objective 5.

Efficiency/ Impact on economy, competitiveness, competition and SMEs

The Option 2 scenario would have a positive impact on EU's competitiveness and SMEs as it allows for creating a mechanism fostering Member States' and Union's cybersecurity

research and innovation capacities.

- This option allows creating synergies and pooling resources to invest in necessary capacities at the Member States' level or develop European shared assets (e.g. by jointly procuring necessary cybersecurity testing and experimentation infrastructure). These assets could be used by researchers, industries and SMEs across different sectors for research and development purposes. This effort is likely to result in increased access of SMEs and industries from different sectors to such facilities, which will stimulate innovation. This will also cut costs for some demand businesses, who would not have to either invest in their own testing facilities or look for them outside Europe. However the efficiency gains under this option are limited as the capacities should serve only research and development processes and not e.g. turning prototypes into real products that could be directly deployed across the market.
- As in Option 1, allowing Member States to make investment economies thanks to coordinated efforts with other interested Member States;

As an entity limited to supporting research and innovation does not allow for activities directly supporting the market deployment of cybersecurity products and solutions, its impacts on helping the industry overcome the current market barriers and increasing their market share would be substantially limited.

Europe would also not be able to take economic advantage of the dual-use market opportunities as such an entity is not the right instrument to encourage defence and civilian cooperation on shared challenges.

This option is also likely to add-value to the national efforts of addressing cybersecurity skills gap to a limited extent as it does not envisage the possibility of going beyond research activities for skills development.

At the EU level, this option is also likely to have limited impact on improving coherence and synergies between different funding mechanisms (Digital Europe Program and Horizon Europe and reducing administrative burden of managing different cybersecurity funding programmes.

This option does not foresee new regulatory obligations for businesses. At the same time the businesses and especially SMEs are likely to reduce their costs related to their research efforts.

In conclusion, the Option 2 scenario has a mixed neutral-positive impact on economy, competitiveness, competition and SMEs. This option is likely to contribute to increased competitiveness of European cybersecurity industry although it would not have a direct positive impact on improving its global market position in terms of market share. It is also likely to help Member States get access to the outcomes of cybersecurity research and innovation projects but would not be sufficient to help their wide deployment across key sectors relevant for public domain.

Social and Environmental Impact

This Option is likely to have some positive impact on the social sphere as it would help accelerate the research on the cybersecurity topics of social and environmental relevance. However, this impact is likely to be weaker than in case of Option 1 as this mechanism does not envisage supporting the transition from prototypes to products that could be deployed widely across sectors.

Stakeholder support

As mentioned in the analysis of the impacts of the Option 1 a majority of industrial and research community stakeholders consulted argued in favour of setting up a mechanism allowing the EU to have a coherent cybersecurity industrial policy to stimulate the development of capacities allowing Europe to autonomously secure its economy, society and democracy (see also Annex 2). According to stakeholders, while supporting research and innovation activities is important, it will not be sufficient to achieve the policy objectives outlined.

7 HOW DO THE OPTIONS COMPARE?

This section presents a comparison of the options in the light of the impacts identified. The options are assessed against the three core criteria of effectiveness, efficiency and coherence, as well as taking into account the support expressed by the different stakeholders.

Effectiveness of the instrument

Both an entity based on art. 173 and 187 TFEU and an entity limited to supporting research and innovation would be more effective in achieving the objectives than the baseline scenario. However, an entity only based on Art.187 would not be able to achieve one of key objectives related to supporting market deployment. It is also less effective in reaching 4 out of 5 remaining objectives than the entity described under Option 1.

Impact on economy, competitiveness, competition and SMEs

Both instruments, an entity based on art. 173 and 187 TFEU and an entity only based on Art.187, would have a positive impact as compared to the baseline scenario. However, the impact of an entity only based on Art.187is expected to be much lower than that of the entity based on art. 173 and187 . This is mainly due to the limitation and scope to supporting research and development, which do not allow for market deployment activities and which are crucial to both help Member States shield their economies and societies and for the industry to become global leaders and increase their market share.

An entity limited to supporting research and innovationis also not in a position to best stimulate collaboration between defence and civilian parts of the cybersecurity market as it is an instrument dedicated to the implementation of the Framework Research Programmes, which does include dual use technologies but only with a have civilian application.

Social and environmental impact

Both options are likely to have positive impact on the social sphere. However, also in this case the impact of an entity based only on art.187 would be weaker if compared to entity based on art. 173 and 187 due to the limitation of the scope of its activity to research and development only. The ability to support deployment is likely to generate much higher positive impact as it will allow public authorities and industries across Member States to more effectively prevent and respond to cyber threats by not only having access to research results but actually equipping themselves with more secure products and solutions. This is in particular relevant for the protection of access to essential services (e.g. transport, health, banking and financial services).

Stakeholder opinion

According to the outcome of the consultation and evidence gathering processes (please see Annexes 1, 2, and 4) there is a clear demand for a mechanism allowing the EU to have a coherent cybersecurity industrial policy to stimulate the development of capacities allowing Europe to autonomously secure its economy, society and democracy. Stakeholders are of the opinion that support to increasing industrial and technological capacities should go beyond research and development activities only if Europe is to fulfil the vision outlined by the Heads of States and Governments at the Tallin Digital Summit for Europe to be "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."[94]. Stakeholders emphasised that the key to success will be a well-defined role of the Centre in supporting and facilitating the efforts of the Network and relevant communities and an inclusive, collaborative approach to the network to avoid creating new silos. The structure should also be flexible so that it can be easily adapted given that cybersecurity is a fast-pace environment.

Based upon the impact analysis preformed in Section 6, the following table compares the merits of Options 1 and 2 against the baseline scenario:

Impacts	Option 0 Baseline scenario	Option 1 Entity based on art. 173 and 187 TFEU	Option 2: Entity based on art.187 TFEU only
Effectiveness			
Objective 1 *Effective cooperation mechanism*	**0**	√√√	√√
Objective 2 *Pooling knowledge and resources*	0	√√√	√√
Objective 3 *Supporting market deployment*	0	√√√	x
Objective 4 *Support to attracting investment*	0	√√√	√
Objective 5 *Closing cybersecurity skills gap*	**0**	√√	√
Efficiency/Impact on economy, competitiveness, competition and SMEs	**0**	√√√	√
Social and Enviornmental Impact	**0**	√√√	√
Flexibility to allow different cooperation models with the network of competence centres	**0**	√√√	√√√
Safeguarding Union's interests	**0**	√√√	√√√
Acting as an implementation mechanism for different EU cybersecurity funding sources	0	√√√	x

Table 1: Comparing the impact of the different options. The symbols "√" and "x" indicate respectively positive and negative impacts, the number of the symbols is the net result of the summing-up of the respective individual ratings of the policy option and indicates the magnitude of the change compared to Baseline scenario. For each symbol a maximum a scale 1 to 3 (maximum positive or negative assessment) is used.

[94] Conclusions of the Prime Minister of Estonia Jüri Ratas after the Tallinn Digital Summit, 29 September 2017

The above comparison demonstrates that an EU-wide collaborative effort stimulated by an entity described under Option 1 offers indeed significant added value for the European economy, society and environment when compared to the baseline scenario and Option 2.

8 PREFERRED OPTION

The above analysis has shown that an entity based on art. 173 and 187 TFEU (Option 1) represents the best instrument capable to implement the goals of the initiative while offering the highest economic, societal, and environmental impact and safeguarding the Union's interests.

In summary, the main arguments in favour of setting the European Cybersecurity Industrial and Research Competence Centre supporting the Network as an EU entity based on art. 173 and 187 TFEU are:

- It ensures flexibility to allow different cooperation models with the network of competence centres to optimise the use of existing knowledge and resources including financial tools and other incentives supporting members of the network
- It provides a visible legal, contractual and organisational common framework to structure the joint commitments of the public and private stakeholders coming from all relevant sectors, including defence;
- It allows creating a real cybersecurity industrial policy by supporting activities related not only to research and development but also to market deployment activities (the latter one with the exception of defence area).
- It fulfils all functional requirements of the legal entity to implement the objectives;
- It can act as an implementation mechanism for different EU cybersecurity funding streams under the next Multi-annual financial framework (Digital Europe Program, Horizon Europe) and enhance synergies between the civilian and defence dimensions of cybersecurity in relation to the European Defence Fund
- It has a positive impact and highest estimated effectiveness of achieving all specific objectives.

Apart from being supported by stakeholders (see previous sections and Annex 2 on Consultation outcomes) this option is also in line with the report of the Estonian presidency on partnerships, which emphasised that in order to reach a higher level of impact "the partnership instruments should cover a much wider set of activities and modalities than research and innovation only." Among other activities mentioned as likely to make a higher impact were, co-creation with end-users, development and experimentation in large scale real life virtual and physical platforms, mission oriented research, deployment activities.[95]

The administrative burden of establishing the network and the Centre is explored in the Annex 3.

9 HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

[95] https://www.hm.ee/sites/default/files/eu_ri_partnerships_final_report.pdf

Monitoring will start with the establishment of the new legal instrument. An explicit clause to monitor the key performance indicators (KPIs) will be included in the legal instrument. Also, an explicit evaluation and review clause, by which the European Commission will conduct an interim evaluation, will be included in the legal instrument, in order to measure the impact of the instrument and its added value. The European Commission will subsequently report to the European Parliament and the Council on its evaluation. Following this evaluation, the Commission may propose a review and extension of the Competence Centre and Network's mandate . The Commission Better Regulation methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted, expert discussions, studies and wide stakeholder consultations.

The Executive Director of the legal entity should present to the Governing Board an ex-post evaluation of European Industry and Research Competence Centre's and Network activities every two years. The legal entity should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress bi-annually to the Commission. The Governing Board should be responsible to monitor the adequate follow-up of such conclusions.

Alleged instances of maladministration in the activities of the legal body may be subject to inquiries by the European Ombudsman in accordance with the provisions of Article 228 of the Treaty.

The list of KPIs that could be used to monitor progress towards meeting the objectives, impact and success of the entity is as follows:

- Number of cybersecurity infrastructure/tools jointly procured.
- Access to testing and experimentation time made possible for European researchers and industry across the Network and within the Centre. Whenever the facilities already exist, increased number of hours available for those communities in comparison to the hours currently available.
- The number of user communities served and number of researchers getting access to the European cybersecurity facilities increases when compared to the number of those having to look for such resources outside Europe.
- Competitiveness of European suppliers starts increasing, measured in terms of global market share (target 25% market share by 2027), and in terms of share of European R&D results taken up by industry.
- Contribution to next cybersecurity technologies, measured in terms of copyright, patents, scientific publications and commercial products.
- Number of cybersecurity skills curricula assessed and aligned, number of cybersecurity professional certification programmes assessed;
- Number of scientists, students, users (industrial and public administrations) trained.